

Get to Know the Cobalt Core

Answers to the most frequently asked questions
about our global community of experienced,
curated, and collaborative pentesters



Table of Contents

What Is the Cobalt Core?	2
Finding and Selecting Members of the Cobalt Core	5
Assigning the Right Pentesters for Success	7
How Does Cobalt Pick the Right People for the Test?	8
How Many Pentesters Work on a Project?	9
How Are Customers Introduced to the Pentesters?	9
Testing, Finding, and Reporting Vulnerabilities—the Cobalt Way	10
What Happens When Pentesters Find a Vulnerability?	10
How Can Customers Follow What the Pentesters Are Doing?	12
What Happens if Tested Assets Change During the Pentest?	13
Maximizing the Remediation and Retesting Process	14
Do Pentesters Help With Remediation?	14
How Do Customers Signal That a Fix Is Ready For Retesting?	15
Sharing Feedback and Requesting Specific Pentesters for New Projects	16
How Do Customers Share Feedback on the Pentesters and Overall Experience?	16
Can Customers Request the Same Pentesters for a Later Project?	17
Why Experts Choose the Cobalt Core	18

What Is the Cobalt Core?

When you engage [Cobalt's Pentest as a Service platform](#), you tap into a carefully curated and thoroughly vetted international community of pentesters—the Cobalt Core. Your business will benefit from high quality talent, dynamic testing, and streamlined collaboration—all at a caliber to match your tech stack and teams. That's why we're providing a closer look at our experts and the processes they follow, including:

- Who makes up the Cobalt Core and how they are vetted.
- How we assign the right pentesters to your projects and set them (and you) up for success.
- How the Cobalt Core tests, finds, and reports vulnerabilities with complete visibility for you.
- How we maximize the retesting and validation process.
- How to share feedback and request talent on your next project.



Vinod Tiwari
Security engineer at Amazon
9+ years experience

Martin Hansen
IS Consultant at Norlys Bank
10+ years experience in IT security and QSA

Robert Kugler
10+ years of security experience
Helped strengthen the security of PayPal and Spotify

In less than ten years, the Cobalt Core has secured more than 3,000 assets, including web and mobile applications, APIs, networks, and cloud instances. We draw from a carefully curated community of over 300 testers crossing six continents, with the majority of our Core living in the United States, India, the United Kingdom, Romania, and Germany. Curiosity, problem-solving, collaboration, and professional development are the main reasons pentesters hope to join the Cobalt Core. Here's what a few of our Core members had to say about working for Cobalt and ultimately, for our customers:



"Without a doubt, my main motivation is the challenge itself. Each pentest is a personal challenge that I take very seriously, and find extremely fun at the same time. At the beginning of my career my motivation was somewhat different. When you are a woman in a predominantly male sector you want acceptance and respect from your colleagues. In a pentest, that can be achieved with good findings. When you grow professionally and gain confidence in yourself, fears disappear and that's when you enjoy your work the most."

Martina Matarí
COBALT CORE PENTESTER

[CHECK OUT MARTINA'S PENTESTER SPOTLIGHT →](#)



"I enjoy working with like-minded offensive security professionals. It is amazing that Cobalt allows me to collaborate on interesting projects, meet people from around the world, and work on unique and challenging architectures. Cobalt encourages this collaborative environment and helps foster a community centered on learning. When you are a part of the Cobalt Core, it feels like you're part of a bigger team."

Stefan Nicula
COBALT CORE PENTESTER

[CHECK OUT STEFAN'S PENTESTER SPOTLIGHT →](#)



“The best part about being in the Cobalt Core is the environment of mutual knowledge sharing. I enjoy being able to connect with top pentesters from around the world and learn from them and their findings. You can simply throw out a question in the channel and whoever knows it readily shares their insights to help you out.”

Nikhil Srivastava
COBALT CORE PENTESTER

[CHECK OUT NIKHIL'S PENTESTER SPOTLIGHT →](#)

COBALT CORE STATS

62%

have at least five years of professional pentesting experience.

81%

hold at least one security certification.

60%

hold the Offensive Security Certified Professional (OSCP) certification from Offensive Security.

Certifications

include OSCP, PWSP, CERP, CEH, CPISI, ISO27001L, CISSP, eWPT, MCSA

Finding and Selecting Members of the Cobalt Core

1 APPLICATION

With a sense of what drives members of the Cobalt Core, let's review our identification and vetting process—the first steps to becoming part of the Cobalt Core. We constantly receive inbound applications to become a Cobalt pentester, along with community and customer referrals. Our community team reviews applications based on tenure, professional and technical skills, and expertise. It's not enough to be a strong hacker; we also look for effective communicators, good collaborators, and a customer-oriented mindset. Only the top 5% of applications are admitted to the Cobalt Core.

2 ASSESSMENT

If an applicant's background meets our requirements, we ask the candidate to complete a technical skills assessment. This is how we assess their technical knowledge base and creative problem-solving abilities. We also review the candidate's reporting skills, which are critical to our customer engagements.

3 VETTING

Once a candidate has successfully completed a skills assessment, they will have a face-to-face interview with a community manager to discuss their background and motivations, along with the Cobalt Core community's expectations. Due to Cobalt's collaborative nature, this is a vital step. The Cobalt Core is best enhanced by team players who are excited to work with and learn from others. The skills assessment coupled with the interview form a rigorous vetting process which identifies talented, motivated, and ethical candidates.

4 VERIFICATION

The final step involves a thorough third-party verification of the pentester candidate. Once this is approved, we gather tax documentation and ask the pentester to sign a robust non-disclosure agreement and Cobalt's terms of engagement.

5 CONTINUOUS EVALUATION

Our process does not end there, however. Even after a pentester is accepted into the Cobalt Core, we continue evaluating their performance. All of our pentesters' work is reviewed by customers, peers, and the Cobalt Pentest Operations team.

Assigning the Right Pentesters for Success

Cobalt teams typically include a Customer Success Manager (CSM), a Pentest Lead, and Pentesters. In the background our Pentest Operations team is committed to keeping everything running smoothly. This powerful combination helps create the most effective, streamlined, and repeatable approach to pentesting. Our customers know what to expect and our pentesters know what to do.

ROLE	FUNCTION
Customer Success Manager (CSM)	Guides customers through the pentest lifecycle and focuses on making the experience seamless, relevant, and engaging. Collects feedback and addresses identified issues as quickly as possible.
Pentest Lead	Leads are entrusted with guiding the pentester team. They review and validate findings, keep the team focused on the project scope, and inform the customer about major updates.
Pentesters	These experts perform the tests. Aside from documenting their findings in detail in our platform, they also engage directly with the customer's security and/or development teams to answer questions, share prevention recommendations, and provide additional support where required.
Pentest Operations	Operations team members select the pentesters who best match required skills and locations/time zones. They work closely with Pentesters and Customer Success Managers to ensure the process, from staffing to report delivery, runs smoothly.

How Does Cobalt Pick the Right People for the Test?

Customer input is critical to a successful engagement. When you initially set up your pentest, the Cobalt platform includes detailed guidance for how to scope it depending on your assets, objectives, and desired coverage level.

The screenshot shows the 'Objectives' step (labeled '2') of a four-step process: Asset (1), Objectives (2), Details (3), and Planning (4). The 'Pentest Objectives' form includes the following fields:

- *TARGET(S)**: A text input field with placeholder text: "Please list all URL(S) of the associated target(s). If you need to add an IP range you may also do so in `Objectives`."
- *METHODOLOGY**: A dropdown menu currently showing "External Network".
- *OBJECTIVE(S)**: A section with "Write" and "Preview" tabs. The text area contains: "Coverage of OSSTMM and SANS top 20 security controls."
- *TEST CREDENTIALS**: Radio buttons for "Yes" and "No".
- INSTRUCTIONS**: A section with "Write" and "Preview" tabs. The text area contains detailed guidance:
 - "In this field you should fill special instructions related to the pentest. General information about the asset (= application/API/Network) should be filled on the asset level instead."
 - A bulleted list of instructions:
 - Highlight any features/areas that you want special attention on in this test e.g. recent releases
 - Specific vulnerabilities that you are most concerned about
 - Special Instructions on how to access the target environment (if any/needed, e.g. if it is an internal network test, you can give info on the jumpbox)
 - Highlight any areas or workflows that are out of scope for this test. Be aware that we do not recommend having an out of scope list.
 - Any concerns/risks in testing the Application/Network that you want the testers to be careful about (especially for

Based on this information, Cobalt pentest architects will source testers who have demonstrated proficiency in the methodologies required, e.g. they can test both web and mobile apps. Talent selection also depends on pentesters' availability and possibly time zone. If the project demands a very niche skill, Cobalt staff will locate a pentester with the required capabilities.

How Many Pentesters Work on a Project?

Two or three pentesters are typically assigned to work on a project, although this number can go as high as 10. Depending on the scope of the test, Cobalt Customer Success Managers recommend the most efficient number of pentesters to complete a thorough assessment.

What does this look like in practice? [Take what Chuck Kesler, CISO at Pendo, had to say:](#)



“Pendo is a complicated product. It takes time to wrap your mind around how it works. But the quality of the results we got from Cobalt was greater than what I had seen in comparable pentests. I felt like they were digging deep, and that’s not something I’ve always seen in the past. Where previously I might have expected two consultants to be assigned to a project, Cobalt brought five pentesters, each with different skills that complemented each other.”

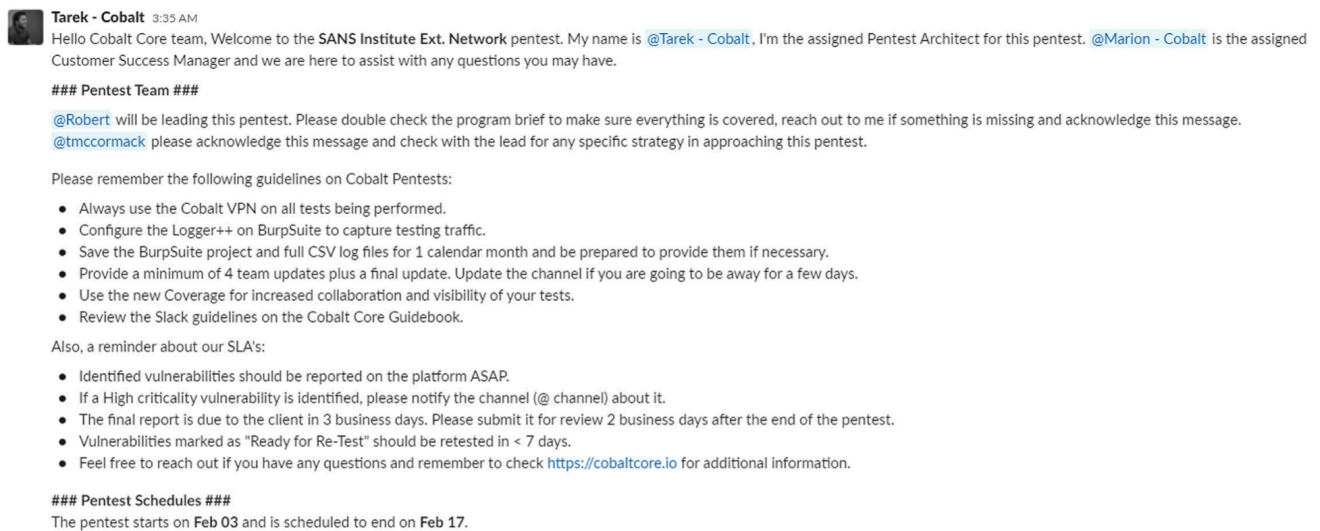
Chuck Kesler
[CISO AT PENDO](#)

How Are Customers Introduced to the Pentesters?

Cobalt team members set up a Slack channel between the customer organization, the selected pentesters, and a Customer Success Manager (CSM) before a test begins. A customer kick-off call is another helpful first step. At this stage, the CSM can highlight inconsistencies or clear up asset descriptions and gather final details needed to start the test. Automated Slack updates are sent to the customer when the test starts, in the middle of the test, and on the last day.

Testing, Finding, and Reporting Vulnerabilities—the Cobalt Way

As soon as all scoping details are resolved, the pentest architect kicks off the test within 24 hours. They outline timelines, SLA reminders for the pentesters, and what to do in certain scenarios. The Slack channel becomes the primary communication method for the next two weeks. Pentesters can ask questions, discuss hypotheses and highlight critical findings—all on Slack.



Tarek - Cobalt 3:35 AM
Hello Cobalt Core team, Welcome to the SANS Institute Ext. Network pentest. My name is @Tarek - Cobalt, I'm the assigned Pentest Architect for this pentest. @Marion - Cobalt is the assigned Customer Success Manager and we are here to assist with any questions you may have.

Pentest Team

@Robert will be leading this pentest. Please double check the program brief to make sure everything is covered, reach out to me if something is missing and acknowledge this message.
@tmccormack please acknowledge this message and check with the lead for any specific strategy in approaching this pentest.

Please remember the following guidelines on Cobalt Pentests:

- Always use the Cobalt VPN on all tests being performed.
- Configure the Logger++ on BurpSuite to capture testing traffic.
- Save the BurpSuite project and full CSV log files for 1 calendar month and be prepared to provide them if necessary.
- Provide a minimum of 4 team updates plus a final update. Update the channel if you are going to be away for a few days.
- Use the new Coverage for increased collaboration and visibility of your tests.
- Review the Slack guidelines on the Cobalt Core Guidebook.

Also, a reminder about our SLA's:

- Identified vulnerabilities should be reported on the platform ASAP.
- If a High criticality vulnerability is identified, please notify the channel (@ channel) about it.
- The final report is due to the client in 3 business days. Please submit it for review 2 business days after the end of the pentest.
- Vulnerabilities marked as "Ready for Re-Test" should be retested in < 7 days.
- Feel free to reach out if you have any questions and remember to check <https://cobaltcore.io> for additional information.

Pentest Schedules ###
The pentest starts on Feb 03 and is scheduled to end on Feb 17.

What Happens When Pentesters Find a Vulnerability?

When pentesters find vulnerabilities, they report them on the Cobalt platform with:

- A detailed description;
- Affected URLs;
- Proof of concept;
- Suggested fix;

VULNERABILITY TYPE

Insufficient Security Configurability > Weak Password Policy

DESCRIPTION

The server does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts. Both the standard user `cobalt-test` and administrative user `admin_user` were observed to utilize weak passwords. This issue was enhanced due to the information leakage issue that describes the password layout in use reported as #PT5686_2

An authentication mechanism is only as strong as its credentials. For this reason, it is important to require users to have strong passwords. Lack of password complexity significantly reduces the search space when trying to guess user's passwords, making brute-force attacks easier.

<https://cwe.mitre.org/data/definitions/521.html>

AFFECTED URL(S)

40.87.83.196

PROOF OF CONCEPT

1. SSH to the target account with the following credentials:
`ssh admin_user@40.87.83.196`
`January2021!`
2. Observe that you are authenticated as the administrative user and have sudo rights.

```
File Actions Edit View Help Kali Docs Kali Forums NetHunter
(kali@kali)~$ ssh admin_user@40.87.83.196
admin_user@40.87.83.196's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1036-azure x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Mon Feb 15 19:13:24 UTC 2021
```

Using integrations with Jira, GitHub or the open Cobalt API, customers can convert these findings into tickets and start working on vulnerabilities right away, even before the full test is complete. Customers can leave feedback or ask questions either in Slack, or within the platform under “Findings,” which sends messages straight to pentesters. If pentesters discover a highly critical vulnerability, they also notify the customer team through the @channel tag on Slack. This enables the customer to act on important findings immediately.

DETAILED FINDINGS EMPOWER CUSTOMERS








“Something I was really impressed with is how responsive pentesters are, not just in how quickly they go. They get back to us pretty quickly, and the answers we get are full, complete, and detailed. When we’re questioning them about something, we get what we’re looking for and the information we need to take that data and then operationalize it on our side.”

Chris Wallace

SECURITY LIAISON ENGINEER AT VONAGE

How Can Customers Follow What the Pentesters Are Doing?

Cobalt Core pentesters follow [coverage checklists](#). They mark completed items as they go so that customers can see what actions have been taken and how the pentest is progressing overall. In addition to the coverage checklist, testers send regular team updates on what they worked on and which tests they’ve completed. Once the pentest is over, the pentest lead pulls all information into a report for review by the pentest architect before uploading it to the platform.

Coverage Checklist		97%
▼ Authentication		100%
▼ Session Management		100%
▼ Access Control		100%
▼ Configuration		100%
▼ Error Handling and Logging		67%

What Happens if Tested Assets Change During the Pentest?

Should an asset change considerably during a pentest engagement, the Cobalt Customer Success Manager will collaborate with the customer and the pentest architect to determine how that affects the pentest's scope and if extra credits will be necessary.

A COBALT CORE PENTESTER EMPHASIZES SCOPE AND COMMUNICATION



“One of the most overlooked aspects in a pentest is having the ability to share ideas, findings, and testing results with the team, including pentesters and the customer. As I’ve learned from Cobalt, a busy pentest comms channel is a happy channel, and strong coverage always pays dividends. A strong scope allows pentesters to focus their efforts and limited time on what truly matters to the customer. In addition, open and active communication helps ensure focus is distributed efficiently across the team, combining ideas and results in order to obtain testing depth.”

Stefan Nicula
COBALT CORE PENTESTER

[CHECK OUT STEFAN'S PENTESTER SPOTLIGHT →](#)

Maximizing the Remediation and Retesting Process

We have designed our pentesting processes so that customers can quickly and easily address vulnerabilities. One defining feature of our Pentest as a Service model is that customers continue to have access to their pentesters even when the testing stage is over, to ask questions or request guidance. More importantly, customers can request a retest to validate the effectiveness of their fixes.

Do Pentesters Help With Remediation?

In addition to including detailed finding information in the platform, pentesters are also available to answer questions throughout remediation in the comments section or on Slack. Questions don't have to come only from the security team—customers can also bring in their engineers to engage directly with pentesters to provide additional support around how to replicate and correct flaws.

CUSTOMERS USE THE COBALT CORE AS AN EXTENSION OF THEIR TEAMS



“We have our Technical Product Managers and we have Development and they work together to understand what our customers need and then build the products that serve those needs. Cobalt partners with both of those sides in order to make sure that when a pentest is done, you are understanding the risk at the product level, so they can make decisions on what will be fixed and when, in tandem with driving new features into our product so that we can meet our customers’ needs.”

Eric Galis

VP COMPLIANCE AND SECURITY AT CENGAGE

How Do Customers Signal That a Fix Is Ready For Retesting?

Once a customer has patched a vulnerability, they can change its status on the Cobalt platform to “Ready for Retest.” When pentesters provide vulnerability reports, it is ideal that customers remediate and change status on the platform to “Ready to Retest” as soon as possible. If some vulnerabilities are left for a year or more before retesting is requested, it is challenging to replicate the same testing methods due to staffing constraints. Customers can also use the platform to [convey that a certain finding does not need further attention](#) because a compensating control is already in place.

As soon as customers flag a vulnerability as “Ready to Retest,” Cobalt pentesters complete the retest within seven days. If a retest reveals that the issue is still exploitable, the pentester changes the status back to “Pending Fix” and provides an explanation for doing so in the platform’s comments section.

HOW FLEXIBLE RETESTING IMPROVES CUSTOMERS’ EFFICIENCY



“Any statement of work that I’ve signed with traditional pentesting allows you the test, you get your remediations, and then you have to wait to retest everything all at once. With Cobalt, they have a sliding window and that’s really useful to the business. I don’t have to wait until all of my remediations are done to get them tested. As soon as one has been released, I can go ahead and have that retested within that window. It really makes us highly efficient to get things out quickly, especially the most critical ones, and we can make sure we’ve done those right. ”

Mandy Huth

[DIRECTOR OF INFORMATION SECURITY AT SMARSH](#)

Sharing Feedback and Requesting Specific Pentesters for New Projects

When the engagement ends, the Cobalt Core Slack channel does not go completely silent.

The pentesters send their last team update as "Tests finalized" and they answer any customer questions regarding the findings or the final report. The channel stays active for the retest period so that security teams and testers can communicate for the retest in case credentials have expired. Channels are archived once all retests are complete and fixes are validated.

How Do Customers Share Feedback on the Pentesters And Overall Experience?

About a week after the pentester team submits its report, Cobalt customers are invited to review their entire pentester group in a survey. We prefer to collect feedback while it's fresh, rather than waiting for remediation to finish. In addition to the survey, customers can also discuss how the group performed in detail on Slack, or in an email and/or feedback call with the Customer Success Manager. This presents an opportunity for customers to share preferences for their next engagements. For example, they may want to work with testers in similar time zones.

Can Customers Request the Same Pentesters for a Later Project?

For subsequent pentests, sometimes it helps to keep the same Pentest Lead who is familiar with the application and has built a knowledge base. On the other hand, new testers offer fresh eyes and new perspectives and techniques.

A lot depends on the applications being tested. Should you want a specific pentester for your next project, we will reach out to check their availability. Please note, however, that specific pentester requests will require some advance planning and cannot be accommodated within 24 hours. If a particular pentester is requested but not immediately available, Cobalt will offer to delay the pentest at the customer's discretion. Cobalt cannot guarantee the same team, but will work towards that if it is the customer's preference. The great news is that the Cobalt Core is never short of talented, collaborative pentesters who love what they do.

Why Experts Choose the Cobalt Core

Cobalt's pentesting service depends on the commitment and dedication of our pentesters, and it is fueled by the collaborative nature of the Cobalt Core. At this point, you might wonder "Why would security experts be interested in joining and staying in the Cobalt Core?"

When we surveyed our pentesters, they shared that the Cobalt Core along with its PtaaS platform provide a cooperative and collegial environment that is unlike any other security platform out there. It provides a space for them to explore interesting applications and learn from their pentester peers and customer security teams alike. Pentesters are able to connect to the Core community via Slack and in-app communication. This collaborative nature has forged a community built around trust, professionalism, diverse expertise, and unique perspectives. Collaboration, combined with the thrill of the hunt, makes for a security professional's ideal work environment. Don't just take our word for it. Here's what our Cobalt Core members have to say:

WHAT MOTIVATES YOU WHEN IT COMES TO PENTESTING?



"Learning about new technologies is my passion and Cobalt gives me the chance to learn from other pentesters. The teamwork dynamic of Cobalt is like no other and allows me to level up my pentesting experience. I am motivated by the community and my passion for the work. Everyday it's my dream job!"

Jesus Arturo Espinoza Soto
COBALT CORE PENTESTER

[CHECK OUT JESUS'S PENTESTER SPOTLIGHT →](#)

WHAT DO YOU ENJOY THE MOST ABOUT BEING A PART OF THE COBALT CORE?



“One other thing that needs to be mentioned is the fact that the Cobalt Core team is united and supportive. Personally, it feels like a family to me, and we constantly share updates from the security space. For example, if a member has a technical question they pose to the community, then in five minutes he or she will already have several answers from members of the community from all over the world.”

Andreea Druga
COBALT CORE PENTESTER

[CHECK OUT ANDREEA'S PENTESTER SPOTLIGHT →](#)

WHAT DO YOU WISH EVERY COMPANY/CUSTOMER KNEW BEFORE STARTING A PENTEST?



The first is to have a clear scope, which means you, as a customer, should have a good understanding of what you want to test and what you don't want to test. In the past, I have seen this happen, a pentester tests something that the customer did not want tested, but it was not communicated ahead of time. In the end, neither side is happy, the pentester wasted their time on something that the customer didn't want. Remember, communication is key!

Something that can also be extremely beneficial for a pentest engagement is having a skilled blue team or blue teamer involved during the test. It can be difficult to communicate technical details to people if they do not fully grasp security.

Valerio Brussani
COBALT CORE PENTESTER

[CHECK OUT VALERIO'S PENTESTER SPOTLIGHT →](#)

What's Next?



IF YOU'RE A CUSTOMER

Reach out to your Customer Success Manager with feedback or additional questions.



IF YOU WANT TO KNOW MORE ABOUT OUR PLATFORM

Review the different features our platform can offer to your team.

[SCHEDULE A DEMO →](#)



IF YOU WANT TO READ MORE ABOUT OUR PENTESTERS

Check out our suggested further reading:

[“Pentester Panel: Lessons from the Frontlines”](#)

[“Pentester Diaries Ep1: Understanding Business Logic”](#)

[“Exploring Valuable Pentester Traits: Top Cobalt Core Pentesters of 2020”](#)

[Join the Cobalt Core →](#)