

BLAZE

SOC2

Penetration Testing and Vulnerability Scanning Guide

Blaze Information Security

2024



WHO WILL BENEFIT FROM THIS GUIDE?

We created this guide to bring relevant information on the topic of penetration testing and vulnerability scanning for SOC 2 audits for leaders in the following audiences:

- Executives responsible for IT security in an organization
- (CISO, VP of security, CIO)
- Upper-level management, such as C-level executives
- (CEO, CTO, COO, CFO)
- Senior members of an audit team and audit committees
- Compliance managers
- Cybersecurity engineers and analysts
  (AppSec, SecOps, InfraSec, etc.)
- Engineering managers and product owners

TABLE OF CONTENTS

Introduction 04

What is SOC 2 compliance? 05

Are penetration testing and vulnerability scanning required for SOC 2 compliance? 07

What is SOC 2 penetration testing? 08

How to define the scope of a penetration test? 09

What security testing methodologies suit a SOC 2 pentest? 10

What is the duration and cost of a SOC 2 penetration test? 11

How often should I conduct a pentest for SOC 2 compliance? 13

What is vulnerability scanning? 14

Pros and cons of vulnerability scanning 16

Penetration testing vs. vulnerability scanning in the context of SOC 2 17

How to select a reputable penetration testing firm? 18

INTRODUCTION

Achieving SOC 2 is now an essential step for many companies, especially those operating in the SaaS space, to prove to third parties that they have robust procedures to safeguard data and information systems, particularly in the cloud. In many cases, presenting a SOC 2 report can determine whether or not a deal will go through, underscoring its importance to many organizations as it directly impacts revenue and trust in your organization.



The idea for creating this guide came up from the realization that many organizations that engaged with us in the past at some point found themselves in a situation where they needed to perform penetration testing as part of their SOC 2 audit but struggled to find informative and accurate guidance.

This guide attempts to answer the most frequently asked questions related to SOC 2 and penetration testing that we collected from these interactions and help buyers make a more informed decision when selecting services and picking a cybersecurity company to support their compliance objectives.



WHAT IS SOC 2 COMPLIANCE AND WHY IS IT IMPORTANT?



The **SOC 2 framework** was developed by the American Institute of Certified Public Accountants (AICPA), providing a comprehensive set of guidelines for companies that handle sensitive information.

SOC 2 compliance refers to standards organizations must meet to ensure appropriate controls for protecting sensitive data. The framework includes five principles:

- Security
- Availability
- Confidentiality
- Privacy
- Processing integrity

Organizations must implement the appropriate controls to meet these principles to be compliant.

To become SOC 2 compliant, an organization must undergo a rigorous audit process and demonstrate that it has adequate controls to effectively protect customer data and other sensitive information it may handle.

SOC 2 compliance has become increasingly important in recent years as data breaches have continued to rise. Many organizations now require their service providers to be SOC 2 compliant to protect their customers' data. While achieving compliance can be challenging, it is essential for any company that handles sensitive information, especially for SaaS companies that operate in the cloud.

By meeting the highest standards for security, integrity, privacy, and confidentiality, SOC 2-compliant organizations can give their customers peace of mind knowing that their data is handled securely, backed by numerous procedures and by industry best practices.

THE DIFFERENCES BETWEEN SOC 2 TYPE I AND TYPE II

Two types of AICPA SOC 2 attestation reports are SOC 2 Type I and Type II. The difference between them is the following:

- **SOC 2 Type I:** reports on an organization's information security controls at a specific time. The idea is to identify the controls and whether they are fit for purpose and in place.

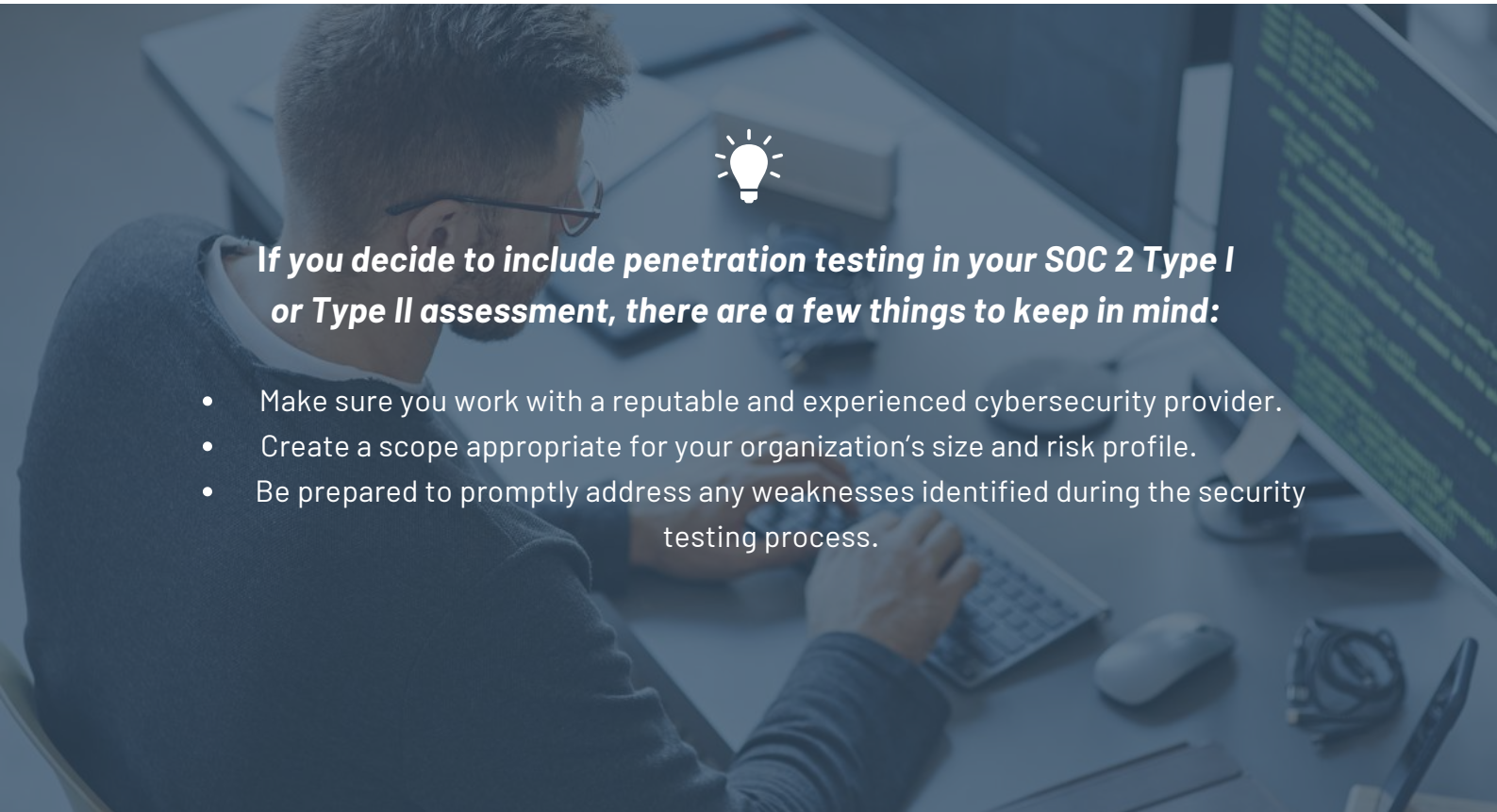
- **SOC 2 Type II:** reports on an organization's security controls over a period of time (3-12 months). The main goal is to determine whether the controls work as intended and fulfill the requirements of AICPA's Trust Services Criteria. They are more comprehensive and valuable for customers assessing an organization's long-term commitment and strategy regarding cybersecurity.

SOC 2 TYPE I



SOC 2 TYPE II





If you decide to include penetration testing in your SOC 2 Type I or Type II assessment, there are a few things to keep in mind:

- Make sure you work with a reputable and experienced cybersecurity provider.
- Create a scope appropriate for your organization's size and risk profile.
- Be prepared to promptly address any weaknesses identified during the security testing process.

ARE PENETRATION TESTING AND VULNERABILITY SCANNING REQUIRED FOR SOC 2 COMPLIANCE?

The answer is simple: penetration testing is not mandatory to achieve SOC 2 compliance. However, auditors often recommend pentesting assessments to augment the audit and fulfill certain items in Trust Services Criteria (Monitoring activities). Whether or not to include it in your assessment is a decision that should be made based on your organization's specific needs, threat profile, and risk appetite.

Nevertheless, the Trust Services Criteria sections CC 4.1 and CC 7.1 of the AICPA advise companies undergoing SOC 2 to consider various types of cybersecurity assessments, such as pentesting and vulnerability scanning:

- **COSO Principle 16:** "The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning."
- **CC4.1** point of focus – "Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certifications made against established specifications (for example, ISO certifications), and internal audit assessments."
- **CC7.1:** "To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities"
- **CC7.1** point of focus: "Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis"



Several organizations and auditors find that pentests and regular vulnerability scans can enhance audits and help achieve compliance. Additionally, these measures offer the extra advantage of bolstering the company's cyber defenses.

There is a mention of pentesting in the criteria, suggesting that it can be one of the methods to perform the required evaluations. Still, an auditor may say that your organization's current ISO 27001 certificate is enough to fulfill the requirements, for example. In our experience, even a customer's public bug bounty program was once accepted by an auditor as evidence to meet CC4.1. It is all open to interpretation, but there is no doubt that penetration testing is a crucial step to satisfy this requirement, with the added benefit of discovering risks your organization might be exposed to and improving your resilience against cyber attacks.

WHAT IS SOC 2 PENETRATION TESTING?

Also known by the short form "pentest," penetration testing involves a simulated attack using the same tools, tactics, techniques, and procedures as an adversary for purposes of ethical security testing. The intention is to identify vulnerabilities and exploit weaknesses to compromise and demonstrate impact on a particular system, a network, or an entire organization.

A pentest assessment can be conducted using a variety of approaches, each of them taking into account a different point of view:

01 BLACK-BOX

In black-box testing, the pentester has no prior knowledge of the system or application under test. Security vulnerabilities are identified from the point of view of a complete external attacker.

02 GRAY-BOX

This type of testing is a blend of black-box and white-box testing. In gray box testing, the tester has some limited knowledge of the system or application under test. This might include high-level information about the system's architecture, data flows, and test credentials. No source code access is given.

03 WHITE-BOX

In this approach, the security engineer has complete access to the source code, blueprints, and design of the system under test. This allows the pentester to identify security vulnerabilities that may not be apparent from observing the system's behavior from an outside perspective.

Most professional pentesting firms will advise against a pure black-box perspective. Sometimes systems are a tough nut to crack from the outside, but with authenticated access, even on a basic permission level, security may be far below optimal. **Our experience is that gray-box testing is the preferred approach for most SOC 2 penetration testing engagements.**

The client typically determines which systems or applications are to be assessed and what types of tests are to be conducted.

We feel it is important to highlight that in the context of SOC 2 compliance, there are no significant differences between penetration testing for SOC 2 and for other purposes or compliance requirements.

What are the benefits of performing penetration testing for SOC 2 compliance?

Despite not being required for SOC 2, pentests can be helpful for various reasons beyond simply being compliant with a security framework.

A thorough pentest assessment can provide valuable insights into an organization's cybersecurity posture and identify weaknesses in an organization's defenses by simulating an attack. Pentests can play an essential role in helping organizations to improve their cybersecurity, comply with regulatory compliance requirements and satisfy vendor risk assessments.

Penetration tests can be augmented using automated tools, but skilled and professional pentesters will go beyond automation and conduct manual tests. Although more labor-intensive, they often find hidden security vulnerabilities that automated tools would miss. Automation is suitable for routine tasks, such as scanning for open ports or probing for known vulnerabilities. Still, it is not yet fit to replace an experienced ethical hacker well-trained to identify vulnerabilities and risks.



The scope of a pentest outlines the boundaries of the engagement, which often entails a list of assets the pentesting team is allowed to attack while excluding assets that are not supposed to be attacked. Undoubtedly, defining the scope of a penetration test can be a tricky process. After all, the whole point of a pentest is to find vulnerabilities that an attacker could exploit. As such, it's vital to ensure that the scope of the test is broad enough to identify potential threats but not so broad that it becomes hard to manage or cost-prohibitive.

From our experience, organizations undergoing SOC 2 compliance usually have the following in mind for their pentest scope:

- The company's flagship product, user-facing SaaS platform
- APIs *(REST, GraphQL)* and microservices
- Security testing of mobile apps, if applicable
- Any administrative panel or back office behind the user-facing SaaS
- Internet-facing server infrastructure *(usually cloud-hosted)*
- The company's internal network, servers, key infrastructure such as Active Directory, Kubernetes clusters, etc.

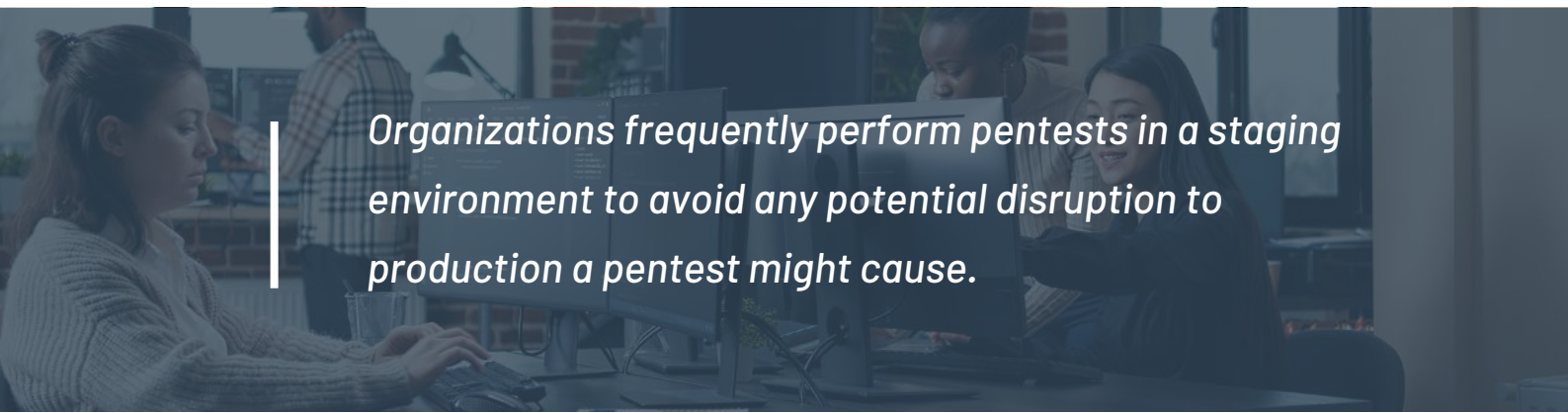
→

Organizations frequently perform pentests in a staging environment to avoid any potential disruption to production a pentest might cause. As long as your staging environment is close to production, this is an acceptable and popular approach. Nevertheless, before engaging a pentest, it is advisable to ask your SOC 2 auditor if they feel this approach is acceptable.

WHAT SECURITY TESTING METHODOLOGIES SUIT A SOC 2 PENTEST?

The methodology used will depend on the specific goals of the test. With the added factor that SOC 2 does not define exact guidelines for penetration testing and the procedures that should be used, it is often left open to interpretation.
However, a few standard methodologies are often used in SOC 2 penetration testing. One of the most popular is the OWASP Top 10. This methodology focuses on the most common web, API, mobile, and even IoT security risks, making it a perfect choice for organizations looking to identify and address potential threats. Combining OWASP Top 10 with OWASP Testing Guide should satisfy nearly all pentest requirements for SOC 2 audits.

Other popular methodologies include SANS 25, OSSTMM, and PTES, which go beyond application security but include network security too. Finally, the NIST 800-115 methodology can also be used in compliance pentests. This methodology focuses on identifying and assessing risk, making it a good choice for organizations that want a comprehensive view of their security posture.



Organizations frequently perform pentests in a staging environment to avoid any potential disruption to production a pentest might cause.

WHAT IS THE DURATION AND COST OF A SOC 2 PENETRATION TEST?

How long does a SOC 2 penetration test assessment take?

The duration of an average SOC 2 pentest engagement is **between 5 to 25 person days**, depending on the scope of the assessment.
A pentest of a single website or web application might take only a few days. In contrast, a comprehensive pentest of an extensive network or a complex SaaS platform could take several weeks. Most pentests, especially for SaaS companies, can be completed within a little over a week or two but can exceed this estimate when a larger scope is defined.

Buyers should be suspicious of providers offering "express" pentests that only last one, two, or three days. These "pentests" are most likely performed almost exclusively using automated scanners, or at best, they blindly follow a basic pentest checklist without any adversarial mindset or creativity. In such situations, there's a good chance subtle vulnerabilities, especially those pertaining to an application's business logic, were missed.
A good rule of thumb is that any pentest for SOC 2 performed under 40 hours for a small to medium-sized scope means there was not enough time for a pentester to manually inspect your systems and turn over every stone as it should.



How much does SOC 2 penetration testing cost?

On average, the price of a penetration test assessment for SOC 2 performed by a reputable and accredited cybersecurity firm will fluctuate between **$8,000 and $25,000**. However, the cost of a SOC 2 penetration test can vary depending on the scope size and complexity.
In some cases, the cost may be even higher if the organization requires a more comprehensive assessment or lower for a small scope. Many reputable pentest providers start at a ballpark figure of $250 to $300 per hour – with niche and specialized work, such as product security assessments or reverse engineering, having a higher hourly price tag (but these are rarely in scope for SOC 2 pentests).

→



→

Buyers should be suspicious of providers charging dramatically low prices: most likely, they perform the bulk of the work using automated scanners, which often yield false positives and miss high-risk issues or have unqualified staff to deliver pentest assessments.

While these low-quality pentest reports may sometimes be sufficient to satisfy an auditor, they bring a false sense of security. They can leave your systems vulnerable to attacks, as the assessment probably only scratched the surface.

Average penetration testing pricing

$250 - $300	PER HOUR
$1 600 - $2 500	PER DAY
£800 - £1 300	PER DAY
$1 500 - $2 400	PER DAY
$1 400 - $2 000	PER DAY
€1 200 - €1 700	PER DAY

Ultimately, the cost of a penetration test is a small price to pay for the peace of mind that comes with knowing your systems are secure and achieving your SOC 2 compliance goals.

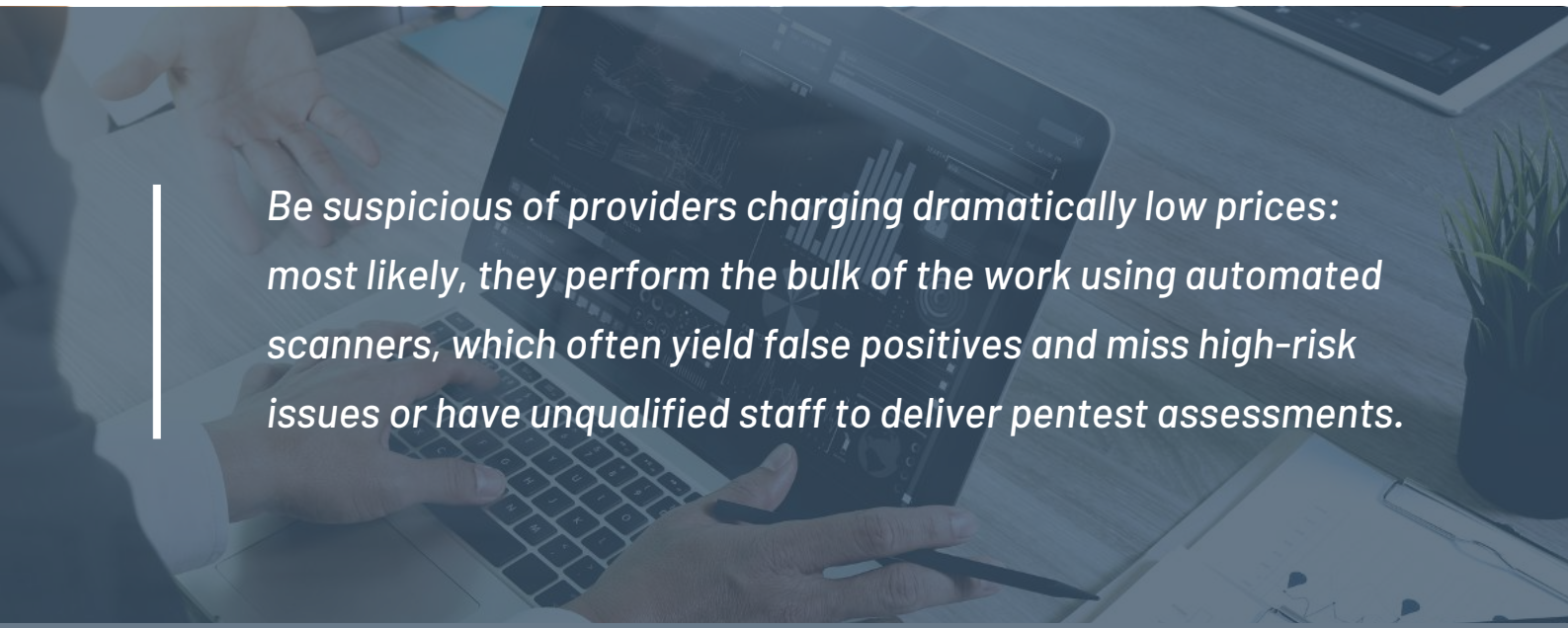
Factors that affect penetration testing costs

Company reputation, certifications and experience of the testing team

Scope size and complexity of the project

Compliance and industry-specific requirements

Retesting and remediation support



> *Be suspicious of providers charging dramatically low prices: most likely, they perform the bulk of the work using automated scanners, which often yield false positives and miss high-risk issues or have unqualified staff to deliver pentest assessments.*

HOW OFTEN SHOULD I CONDUCT A PENTEST FOR SOC 2 COMPLIANCE?

Most organizations undergo SOC 2 audits annually, meaning the reports are valid for 12 months. If your organization follows this cycle of audit, **penetration testing for SOC 2 should be conducted at least once a year** to ensure a strong company's security posture and continuous compliance.

However, there are service organizations that are audited every six months, and it is recommended that your pen test requirements should align with this shorter timeframe.

ONCE A YEAR OR EVERY SIX MONTH



What to expect from a SOC 2 penetration test report?

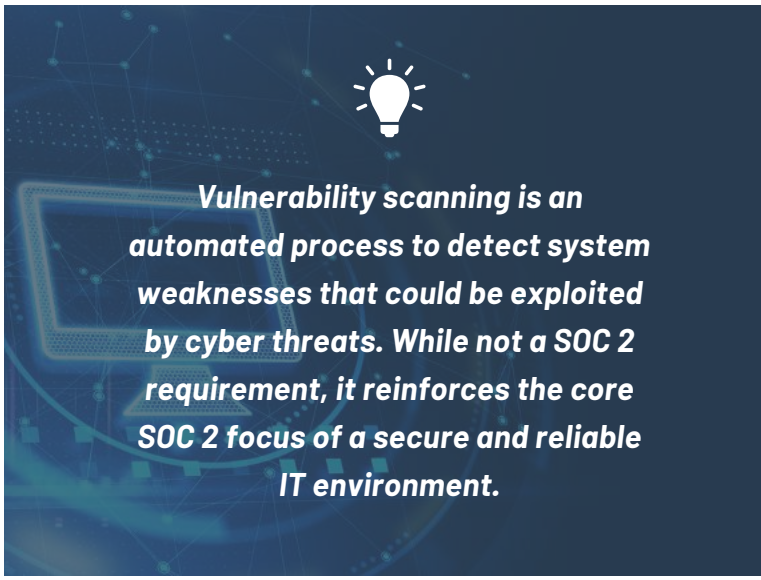
A penetration test report is the main deliverable of a pentest assessment. The document usually contains elements such as the following:

- A high-level summary of the findings
- An executive summary explaining the risk and impact of each vulnerability for non-technical audiences
- Scope, testing methodology, and duration of testing
- Detailed information about the vulnerabilities discovered during testing
- Recommendations for fixing each issue or mitigating their respective risk.

A pentest report should provide a comprehensive analysis of the results of the findings encountered during the assessment, with a clear and concise explanation of the impact and likelihood of an attack.

WHAT IS VULNERABILITY SCANNING?

Vulnerability scanning is a systematic approach to identifying, quantifying, and ranking the vulnerabilities in a system. It's a cyber health check for your IT infrastructure, designed to uncover any potential weaknesses that could be exploited by attackers.
By identifying these vulnerabilities, organizations can address and patch them before they are exploited, significantly reducing the risk of a security incident. Vulnerability scanning should be done on a regular basis, as new vulnerabilities are continually discovered and added to the databases used by scanners.



What are vulnerability scanning requirements for SOC 2 compliance?

Vulnerability scanning is not an explicit requirement in SOC 2 audits but serves as a substantial adjunct to the framework. It adds depth to your organization's security practices and provides demonstrable evidence of proactive measures against potential cyber threats.
Even though it's not a compulsory requirement, vulnerability scanning can aid in fulfilling the subsequent prerequisites criteria CC7.1 from the *Trust Services Criteria* (System operations) and its points of focus:

- **CC7.1:** *"To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities"*
- **CC7.1 point of focus**: "Conducts Vulnerability Scans — *The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis*"

SOC 2 standard mandates that organizations implement effective controls to ensure system and data security to safeguard customer data. Hence, the incorporation of vulnerability scanning in the security strategy can be perceived as a proactive step in meeting SOC 2 compliance security requirements.

While vulnerability scanning is an integral part of cybersecurity, it should not be confused with penetration testing. The two are related but serve different purposes.

How vulnerability scanning can enhance SOC 2 Trust Service Principles



Vulnerability scanning's value lies in its potential to augment the five trust service principles of SOC 2. Here's a closer look at how vulnerability scanning intersects with each of these principles:

- **Security:** Vulnerability scanning is a crucial tool for detecting and addressing system vulnerabilities, helping organizations demonstrate their commitment to a secure environment.
- **Availability:** Regular vulnerability scans identify threats that could lead to denial of service attacks, causing system downtime, thereby ensuring consistent system functionality and accessibility.
- **Processing Integrity:** While not directly tied to vulnerability scanning, system processing integrity can indirectly benefit from it. Scanning helps prevent unauthorized data modifications, supporting accurate and timely data processing.
- **Confidentiality:** By spotting weaknesses that could lead to unauthorized access to confidential data, vulnerability scanning bolsters data confidentiality.
- **Privacy:** Vulnerability scanning identifies system vulnerabilities that could compromise privacy, ensuring timely rectification and maintaining the protection of personal information.

It's true vulnerability scanning isn't a direct requirement of SOC 2; however, it's easy to see how it clearly supports the purpose of SOC 2's trust service principles.

PROS AND CONS OF VULNERABILITY SCANNING

For compliance reasons or not, it's important to weigh the benefits and potential challenges associated with vulnerability scanning. Let's consider both sides of the coin and discuss the benefits and limitations that automated vulnerability scanning can bring.

Benefits of vulnerability scanning

Enhanced security posture:
Vulnerability scanning can identify potential vulnerabilities, and by addressing them, you can greatly enhance the security of your IT environment. Regular scanning enables your organization to stay ahead of potential threats and may help prevent costly and damaging security incidents.

Supports SOC 2 compliance:
Although a vulnerability scan isn't a specific requirement, its practice aligns well with SOC 2's trust service principles. Regular vulnerability scanning can be seen as a demonstration of your organization's commitment to maintaining a secure environment and enhancing trust with your customers and stakeholders.

Risk prioritization:
Vulnerability scanning not only identifies potential threats but can, in some cases, also prioritize them based on their severity to remediate identified deficiencies. This can guide your organization in efficiently allocating resources to address the most serious threats first.

Potential challenges of vulnerability scanning

False positives:
While vulnerability scanners are generally accurate, they can occasionally report false positives, meaning they might identify a threat where there is none. This could lead to unnecessary use of resources in investigating and addressing these supposed threats.

Only scratches the surface:
While vulnerability scanning can identify many potential threats, it isn't a cure-all solution. Some threats may be missed, especially new or emerging ones that aren't yet included in the scanner's database. Additionally, it doesn't have the same contextual use for the vulnerabilities as a pentest will do, making a vulnerability scan less in-depth than a manual pentest assessment led by an experienced security engineer.

Vulnerability overload:
An automated scanner can identify a large number of vulnerabilities, more than an internal security team can effectively manage or remediate in a reasonable time frame, making it difficult to prioritize what to fix first.



PENETRATION TESTING VS. VULNERABILITY SCANNING IN THE CONTEXT OF SOC 2



Penetration testing and vulnerability scanning are essential tools for managing cybersecurity risk, as they can help identify security weaknesses in systems and networks. However, there are critical differences between the two approaches.

Vulnerability scanning is typically automated, while penetration testing is usually manual. Vulnerability scanners can be run frequently to look for new security weaknesses, while penetration tests are typically only conducted occasionally. Scanners identify potential security issues that follow a repeatable pattern, while pentesting involves exploiting vulnerabilities to gain access to systems or data.

In general, penetration testing is more comprehensive and sophisticated than vulnerability scanning. However, both techniques can help manage cybersecurity risk. Organizations should use a combination of penetration testing and automated scanning to get the best possible picture of their security posture.

Several organizations and auditors find that pentests and regular vulnerability scanning can supplement the audit and meet the needs to accomplish compliance with the added benefit of an additional step to increasing their cyber defenses

Some cybersecurity firms may offer automated vulnerability scanning disguised as penetration testing. You must understand the difference between the two and ensure you get the correct service to help with your compliance goals. A "too good to be true" pricing structure may hint at this practice.

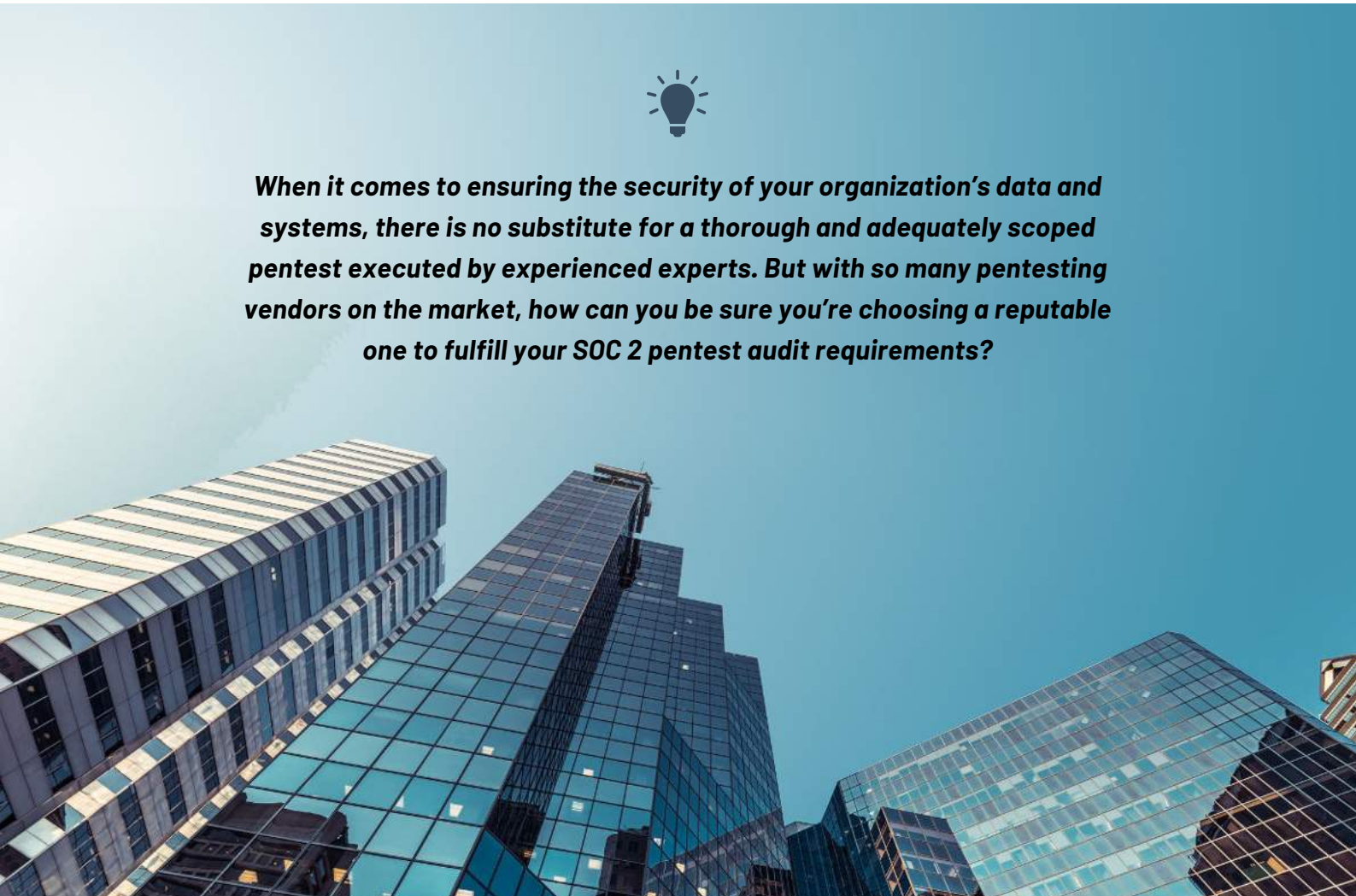
HOW TO SELECT A REPUTABLE PENETRATION TESTING FIRM?

While neither vulnerability scanning nor penetration tests are a mandatory component of SOC 2 compliance, their benefits can make them a valuable addition to your compliance strategy. Providing pentesting reports and evidence of quarterly vulnerability scans will make your audit experience smoother and the auditor confident about your organization's cybersecurity practices.

The decision to incorporate penetration testing and vulnerability scanning should align with your organization's unique needs, risk profile, and resources.

By weighing these considerations carefully, you can make an informed decision that enhances your security posture, supports SOC 2 compliance, reinforces trust with your stakeholders, decreases cyber risks and ultimately shows proactive measures, as well as detection and monitoring procedures to prevent data breaches.

If you decide to go ahead with these services to augment your audit, selecting a reliable service provider becomes crucial.



When it comes to ensuring the security of your organization's data and systems, there is no substitute for a thorough and adequately scoped pentest executed by experienced experts. But with so many pentesting vendors on the market, how can you be sure you're choosing a reputable one to fulfill your SOC 2 pentest audit requirements?

Here are a few things to look for:

- A reputable pentesting vendor should have a proven track record with experience pentesting similar organizations to yours.
- Working with a provider specializing in cybersecurity services can be beneficial as they often provide superior pentest services.
- Qualified penetration testing firms usually have a technical blog, Github, or other channels displaying their technical expertise and research.
- Ensure the vendor has adequate liability insurance to cover damages if something goes wrong during the pentest.
- The vendor's staff should be full-time employees rather than freelancers, and they should have robust security procedures protecting your data during the test.



10 main tips for choosing a penetration testing company



By following the guidelines above, you can be confident that you're choosing the right penetration testing partner.



HOW CAN BLAZE HELP YOUR ORGANIZATION WITH SOC 2 COMPLIANCE AND PENETRATION TESTING?

BLAZE

Here at Blaze Information Security, we are experts in offensive cybersecurity. From the senior leadership to the security consulting team, we're all ethical hackers who believe in technical excellence.

Our service portfolio is composed almost exclusively of penetration testing and application security services. Blaze's team routinely publishes original research in our Labs, and we constantly deliver penetration testing assessments focused on SOC 2 for many customers across North America, Europe, and beyond.

On top of that, we have partnered with two leading compliance automation platforms to provide our customers with full support in their SOC 2 journey. If your company is considering penetration testing or vulnerability scanning as part of your SOC 2 audit process, contact us to discuss your needs.

Contact us for your SOC 2 pen test requirements or automated compliance needs.



BLAZE

www.blazeinfosec.com

GERMANY
Friedrichstraße 155
10117, Berlin

PORTUGAL
Praça do Bom Sucesso
131/206
4150-146, Porto

BRAZIL
Rua Padre Carapuceiro
968/2006
51020-280, Recife

POLAND
ul. Józefa Sarego 5/4
31-047, Kraków