



**SOC
ANALYST**



**PENETRATION
TESTER**

**WHICH CAREER PATH IS THE
BEST FOR YOU?**



LetsDefend

TABLE OF CONTENTS

- 3** - INTRO
- WHAT DOES A SOC ANALYST DO?

-
- 4** - DAILY WORK ROUTINES
- PROS OF THE SOC ANALYST JOB

-
- 5** - CONS OF THE SOC ANALYST JOB
- REQUIRED SKILLS FOR SOC ANALYST

-
- 6** - AVERAGE ANNUAL SALARY OF SOC ANALYST

-
- 7** - RESOURCES TO BEGIN A SOC ANALYST CAREER

-
- 8** - WHAT DOES A PENETRATION TESTER DO?

-
- 9** - DAILY WORK ROUTINES
- PROS OF THE PENETRATION TESTER

-
- 10** - CONS OF THE PENETRATION TEST JOB
- REQUIRED SKILLS FOR PENETRATION TESTER

-
- 11** - AVERAGE ANNUAL SALARY OF PENETRATION TESTER

-
- 12** - RESOURCES TO BEGIN A CAREER
- FINAL WORDS
-





INTRO

Candidates who want to pursue a career in cyber security should have knowledge of the sub-branch of cyber security that they want to specialize in. In this article, we discuss penetration tester and SOC analyst, two important professions in the industry and explain what employees in both professions do, their daily work routines, what skills they should have, and the positive and negative aspects of the jobs.

WHAT DOES A SOC ANALYST DO?

Although the SOC analyst undertakes different tasks according to the level (L1, L2, L3), we can say that in general, its task is to detect threats to IT assets, take the necessary security measures and make the necessary analysis.



DAILY WORK ROUTINES

A SOC analyst monitors continuously throughout his shift. Along with the monitoring activity, it examines the alerts created by security products and decides whether there is an attack violation and terminates the alert. If the alert is a real attack, it tries to reveal the details of the attack by making the necessary detailed examination on the devices and systems where the alert occurred. After being informed about the attack, it takes the necessary security measures to avoid being affected by the same attack in the next attack attempt. In general, this is the daily routine of the SOC analyst. In addition, it can develop add-ons suitable for the security software it has managed or used, so that attacks can be detected in a shorter time and action can be taken.

PROS OF THE SOC ANALYST JOB

Since the SOC analyst detects the attacks coming to the organization, he/she sees the current attack methods of the attackers in practice and has the opportunity to analyze live systems.



CONS OF THE SOC ANALYST JOB

As SOC analysts detect attacks, they must monitor IT assets in their area of responsibility around the clock. It should always be on the alert and ready to take action against attack attempts. Although it differs in companies operating on a global scale, they generally work in shifts. Irregular working hours can adversely affect analysts' performance.

REQUIRED SKILLS FOR SOC ANALYST

- Computer science basics
- Mastery of security products
- Ability to take quick action
- To be able to use time efficiently
- Ability to work under stress
- Ability to use basic technical knowledge
- Communication and coordination
- Adapting to different shift hours



AVERAGE ANNUAL SALARY OF SOC ANALYST

SOC analyst salaries vary widely but mostly based on experience and some other criterias. According to the data obtained from Glassdoor, experts with the title of SOC analyst in the USA earn an average of \$97,236 annually as of March 2022.

\$98,404 / yr

Total Pay

\$79,193 / yr

Base Pay

\$19,211 / yr

Additional Pay

source: Glasdoor



RESOURCES TO BEGIN A SOC ANALYST CAREER

- [SOC Fundamentals](#)
- [How to Become a SOC Analyst: in 2022](#)
- [How to Prepare SOC Analyst Resume](#)
- [SOC Analyst Career Without a Degree](#)



WHAT DOES A PENETRATION TESTER DO?

The penetration tester detects vulnerabilities in the target system or software by performing security tests of systems and software belonging to IT assets. It performs social engineering attack simulations on organizations by designing social engineering attacks. While performing security tests, it constantly follows up-to-date technologies and creates new attack methods by learning about its security. This includes attack methods within the scope of security tests. In addition to security tests, it detects security vulnerabilities in the application source code by performing source code analysis.

After performing security tests of applications, network devices and IT infrastructures, it creates reports containing detailed information about the findings to be delivered to the customer. In this way, it informs the organization about the vulnerabilities that exist in practice and need to be eliminated, with its offensive point of view and capabilities.



DAILY WORK ROUTINES

The daily work routines of penetration testers may differ depending on the security test they conduct. If a penetration tester works for a consultancy firm, he or she will have clients and will perform security tests for the customers' IT assets at the request of its customers. These security tests may be in a wide variety of areas like security tests for IoT devices, web applications, mobile applications, servers, network devices and industrial control systems. Penetration test experts document the findings by preparing a report at the end of the security tests. Duties other than preparing the report are mostly similar to the duties of a penetration tester who works for a consulting firm.

PROS OF THE PENETRATION TESTER

The penetration tester always works in an environment where it can apply up-to-date attack techniques while performing security tests. It can use its own attack tools while detecting the vulnerabilities of the target system. It encounters new technologies in practice, as it has the opportunity to perform security tests of a wide variety of technologies.



CONS OF THE PENETRATION TEST JOB

While performing security tests, it is not always possible to perform these tests remotely. Some IT infrastructures must be tested on site. Therefore, the penetration tester has to travel a lot for internal network tests. In addition, when reporting the findings at the end of the security tests, the content of the report is higher in direct proportion to the number of vulnerabilities. Preparing this report often requires a great deal of effort because the person to whom the report will be delivered may be an employee who does not have technical knowledge. Technical details should be transferred to the report carefully and clearly so they can provide an effective report on their work. A disadvantage for the penetration tester is that its time is usually short. Security tests should be carried out in a short time, as the usage time of the resources allocated to you by the institution for security tests is very limited. In this case, it is important that the penetration tester is prepared for the security test in advance.

REQUIRED SKILLS FOR PENETRATION TESTER

- Reporting
- Ability to follow up-to-date technology
- Monitoring and implementation of current vulnerabilities
- Communication and coordination
- Ability to prepare necessary tools in security testing
- Having an offensive point of view
- Ability to use limited time efficiently



AVERAGE ANNUAL SALARY OF PENETRATION TESTER

Penetration Tester salaries are also mostly based on experience and having the technical skills like all other tech jobs. According to the data obtained through Glassdoor, experts with the title of penetration tester in the USA earn an average of \$ 107,150 annually as of March 2022.

\$107,644 /yr

Total Pay

\$89,502 /yr

Base Pay

\$18,142 /yr

Additional Pay

Source: Glasdoor



RESOURCES TO BEGIN A CAREER

- https://www.tutorialspoint.com/penetration_testing/index.htm
- [BOOK] – Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press
- [BOOK] – Ethical Hacking: A Hands-on Introduction to Breaking In, No Starch Press

FINAL WORDS

Working environments, salaries and opportunities for SOC analyst and penetration testing expertise vary according to the country of the firm, the individual's own knowledge and the firm itself. What is important for the candidate here is that he enjoys his job and leads a happy business life.