NOVEMBER, 2021

TOP FIVE HIGH-PAYING JOB POSITIONS YOU CAN PURSUE WITH AN ETHICAL HACKING CERTIFICATION

PECB

www.pecb.com

Data is one of the most important assets of any organization, especially those who deal with sensitive data on a daily basis. As organizations embrace digital transformation every day more, they should consider the new threats that come with it: cybercriminals.

According to the FBI, during 2020, as a result of COVID-19, cybercrime increased as much as 400%. In order to ensure safety, organizations need to regularly update their systems and take preventive measures. One of the newest and most efficient forms of protecting data from viruses, malware, and hackers is to use ethical hackers.

Ethical hacking helps identify weaknesses in an organization's firewall or software security. Their unique perspective allows them to detect potential threats before people with malicious intent are able to capitalize on them. This makes ethical hacking a very important asset in the protection of data and software.

TOP FIVE U.S. HIGH-PAYING JOB POSITIONS IN THE ETHICAL HACKING INDUSTRY

The salaries presented in the following slides represent an average that derives from information provided by **PayScale**, **Glassdoor**, and **Ziprecruiter**

1. Cybersecurity Architect

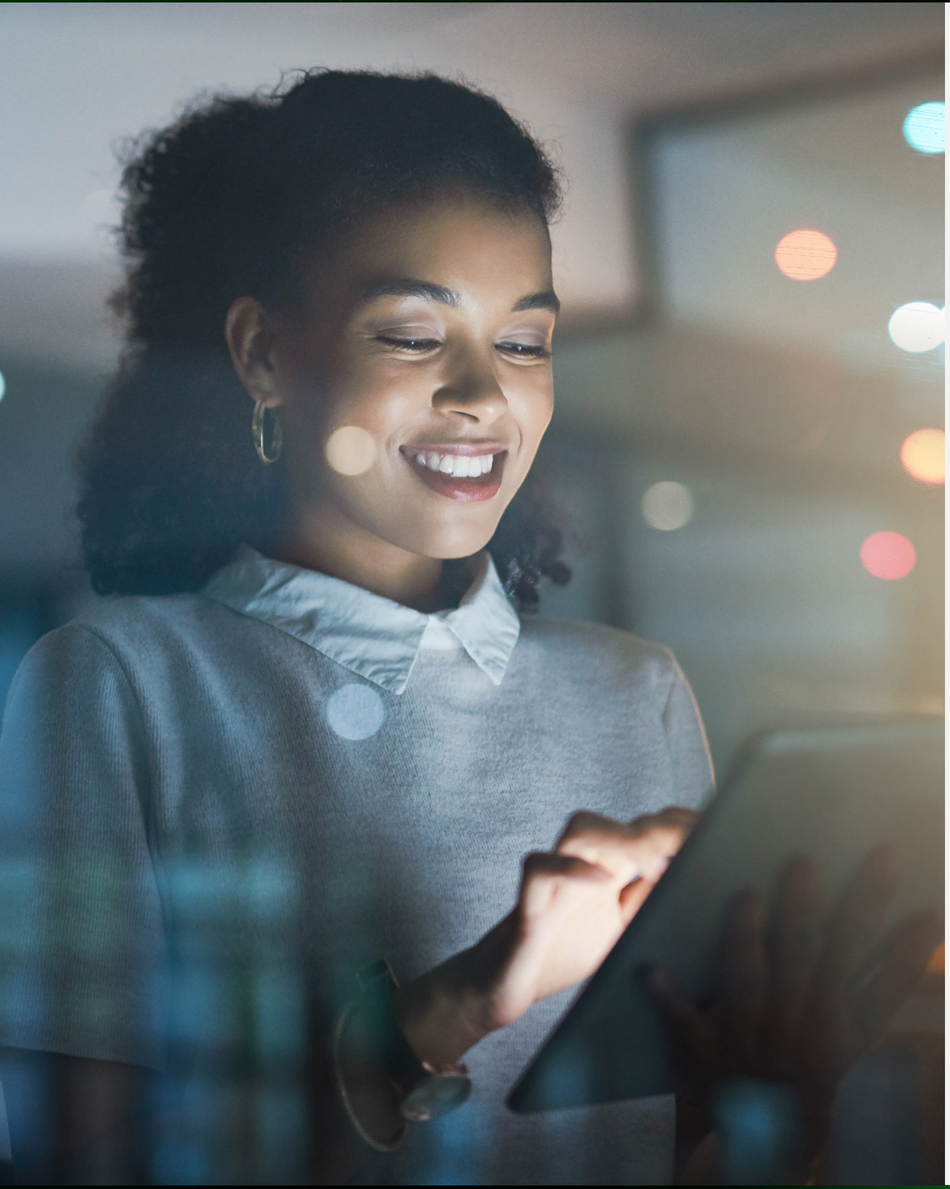
The average salary of a cybersecurity architect is **$132,879 per year.**

A cybersecurity architect is mainly responsible for:

- ✓ Developing an in-depth understanding of the organization’s overall information systems
- ✓ Designing, implementing, and building the systems
- ✓ Aligning an organization’s security strategy with their business technology strategy
- ✓ Identifying the main security threats
- ✓ Identifying security gaps and providing solutions for them
- ✓ Communicating any security and information technology needs to the upper management regularly

Cybersecurity architects should possess technological, administrative, and leadership skills. They should be able to think like a business executive, manage security team members, and communicate effectively with key stakeholders. Certifications in IT security can be a competitive advantage.

2. Cybersecurity Engineer



The average salary of a cybersecurity engineer is **$106,313 per year.**

A cybersecurity engineer is mainly responsible for:

- ✓ Implementing and managing the security measures of an organization’s system and network
- ✓ Testing the system’s vulnerabilities
- ✓ Enabling the proper security controls
- ✓ Responding to all network security breaches
- ✓ Upgrading the security measures
- ✓ Reporting and communicating with relevant departments on a daily basis

Cybersecurity engineers should have experience with advanced persistent threats. They are expected to have outstanding problem-solving skills and an excellent understanding of technology infrastructures.

3. Penetration Tester

The average salary of a penetration tester is **$102,155 per year.**

A penetration tester is mainly responsible for:

✓ Performing network security tests
✓ Writing reports on the tests
✓ Conducting physical assessments of systems and servers
✓ Analyzing security policies and procedures
✓ Reviewing proposed ideas for information security solutions and giving feedback
✓ Staying up to date with the newest security threats

Penetration testers should have knowledge of vulnerabilities and exploits outside of tool suites. They should have knowledge of ethical hacking in general. Ethical hacking certification would be a valuable asset for any candidate.

4. Ethical Hacker

The average salary of an ethical hacker is **$101,140 per year.**

An Ethical Hacker is mainly responsible for:

- ✓ Finding gaps in systems and implement corrective measures to prevent potential attacks
- ✓ Bypassing intrusion prevention systems, intrusion detection systems, firewalls, and honeypots
- ✓ Identifying and fixing sniffing networks, cracked wireless encryption, hijacked web servers, and hijacked web application
- ✓ Creating policies and procedures for reporting issues or notifications

Ethical hackers should have networking skills, computer skills, and programming skills. They should be able to identify general flaws in a system. Ethical hacking certification would be a valuable asset for any candidate.

5. Information Security Analyst

The average salary of an information security analyst is **$90,770 per year.**

An information security analyst is mainly responsible for:

- ✓ Designing and implementing security systems
- ✓ Maintaining security standards
- ✓ Documenting the security breaches
- ✓ Fixing the system's detected vulnerabilities
- ✓ Keeping up to date with the latest IT security trends
- ✓ Researching on security enhancements and proposing IT security recommendations

Information security analysts should possess strong analytical thinking and problem-solving skills. They are expected to assess potential risks and develop possible solutions.

The Certified Lead Ethical Hacker training course enables participants to develop the competence and knowledge required to conduct ethical hacking, mainly for information systems and network penetration tests. Apart from theoretical information, the training course also includes labs that are conducted through a virtual machine. A Lead Ethical Hacker Certification can open the door to different job opportunities.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

CLICK TO SEE HOW PECB CAN HELP

→

☎ +1-844-426-7322

✉ customer@pecb.com

🌐 www.pecb.com

PECB