# Coolest Careers in Cyber

Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in-demand by employers. Which jobs are the coolest and most in-demand? We know; let us show you the hottest cybersecurity jobs for 2021.

## Threat Hunter

- **Why is this role important?**
  - In this role, you’ll be challenged to look at patterns and detect movement from the perspective of someone with malicious intent. Threat hunters can help the security team stay ahead of an attacker by hunting suspicious patterns of behavior that may be indicative of a security threat.

## Red Teamer

- **Why is this role important?**
  - This role allows me to exercise my creativity and to try out new things, to develop new techniques, and to test new products. It is like solving a puzzle that I must continually build upon.

## Digital Forensic Analyst

- **Why is this role important?**
  - Digital forensic analysts are the ones who bring the evidence to light – they’re the ones who research, test, and analyze evidence to help determine the nature of the threat – how it got in, what flaw it exploited, and what it has done, is doing, and potential to do.

## Purple Teamer

- **Why is this role important?**
  - This is a very challenging role, but it’s also a very rewarding role. It’s like being a detective, only instead of trying to figure out who did it, you’re trying to figure out how to stop it.

## Incident Response Team Member

- **Why is this role important?**
  - This job always tests my curiosity and my problem-solving skills. I get to work on a wide range of issues, and I get to work with a great team.

## Cybersecurity Analyst/Engineer

- **Why is this role important?**
  - Cybersecurity analysts/engineers must stay informed about the tools and techniques out there to counter threats and vulnerabilities. This role is critical to protecting the organization's data.

## OSINT Investigator/Analyst

- **Why is this role important?**
  - OSINT investigators and analysts are experts in gathering and analyzing data from open sources to gain insights into potential threats. This role is crucial to ensuring the security of organizations.

## Security Architect & Engineer

- **Why is this role important?**
  - As a security architect, I can see how the security of an organization depends on the security of its systems and services. From my point of view, this is like designing a fortress that an attacker cannot break through.

## Executive

- **Why is this role important?**
  - CISOs respond to incidents as part of a team, with a wide variety of specializations. Ultimately, they must effectively coordinate the plans of the incident responders to ensure the safety and security of the organization.

## Cloud Security Analyst

- **Why is this role important?**
  - Cloud security analysts are responsible for ensuring that cloud-based services are secure and compliant with regulations. This role is critical to protecting an organization's data in cloud environments.

## Intrusion Detection/Prevention (IDS/IPS) Analyst

- **Why is this role important?**
  - Intrusion detection/prevention analysts are responsible for monitoring and analyzing network traffic to detect and prevent intrusions.

## Security Awareness Officer

- **Why is this role important?**
  - Security awareness officers are responsible for educating employees about security best practices and helping them understand the importance of information security.

## Red Teamer - All-Around Defender

- **Why is this role important?**
  - From my point of view, this role allows me to exercise my creativity and to try out new things, to develop new techniques, and to test new products. It is like solving a puzzle that I must continually build upon.

## Blue Teamer - All-Around Defender

- **Why is this role important?**
  - As a blue teamer, I get to exercise my creativity and to try out new things, to develop new techniques, and to test new products. It is like solving a puzzle that I must continually build upon.

## Security Researcher & Exploit Developer

- **Why is this role important?**
  - As a security researcher and exploit developer, I get to exercise my creativity and to try out new things, to develop new techniques, and to test new products. It is like solving a puzzle that I must continually build upon.

## DevSecOps Engineer

- **Why is this role important?**
  - This role combines software development and security, allowing developers to build secure applications from the ground up.

## MedSec Exploitation Analyst

- **Why is this role important?**
  - As a MedSec exploitation analyst, I get to exercise my creativity and to try out new things, to develop new techniques, and to test new products. It is like solving a puzzle that I must continually build upon.

## Malware Analyst

- **Why is this role important?**
  - Malware analysts are responsible for identifying and understanding malware threats, and for developing strategies to mitigate those threats.

## CISO

- **Why is this role important?**
  - A CISO is responsible for developing and implementing effective strategies and controls to protect an organization’s information assets.

## Chief Information Security Officer (CISO)

- **Why is this role important?**
  - The CISO plays a crucial role in protecting an organization's information assets, ensuring that the organization is compliant with relevant regulations and standards, and managing information security risks.

## Application Pen Tester

- **Why is this role important?**
  - Application penetration testers probe the security integrity of a company's applications and networks to identify vulnerabilities.

## In-Depth Pen Tester

- **Why is this role important?**
  - In-depth penetration testers perform a comprehensive analysis of an organization's security posture, identifying vulnerabilities and weaknesses.

## DevSecOps Engineer

- **Why is this role important?**
  - DevSecOps engineers are responsible for integrating security practices into the software development process to ensure that security is built into the system from the ground up.

## Application Pen Tester

- **Why is this role important?**
  - Application penetration testers probe the security integrity of a company's applications and networks to identify vulnerabilities.

## Reverse Engineer

- **Why is this role important?**
  - Reverse engineers perform a detailed analysis of software or hardware to determine how it works, including identifying vulnerabilities that could be exploited.

## Threat Hunter

- **Why is this role important?**
  - Threat hunters are responsible for identifying and investigating potential cyber threats and vulnerabilities.

## Blue Teamer - All-Around Defender

- **Why is this role important?**
  - Blue teamers are responsible for identifying and mitigating potential security threats.

**Recommended Courses Associated**

- **SEC530**
- **SEC508**
- **SEC572**
- **SEC578**
- **SEC509**
- **SEC450**
- **SEC488**
- **SEC537**
- **SEC586**
- **SEC540**
- **SEC555**
- **SEC560**
- **SEC503**
- **SEC564**
- **SEC660**
- **MGT516**
- **MGT551**
- **MGT519**
- **MGT508**
- **ICS612**
- **ICS515**
- **GPEN**
- **GREM**
- **GCIA**
- **GCDA**
- **GCFE**
- **GICSP**
- **GOSI**
- **GSI**
- **GKD**
- **GSA**
- **GSDA**
- **GSAI**
- **GSDA**
- **GDOC**
- **GOSI**
- **GSI**

*Course coming soon. Learn more about the new courses at sans.org/new-sans-courses*