

Trinity A. Salva

Professor Kirkpatrick

CYSE 200T

September 4th, 2025

AI Job Market Analysis Output

I reviewed the spreadsheet you provided, which lists a wide range of cybersecurity-related jobs and the associated skills. From these, I pulled out recurring themes to identify the **most in-demand skills** across cybersecurity job roles.

Synopsis of In-Demand Cybersecurity Skills

Employers consistently seek professionals who combine **technical expertise** (networking, security frameworks, programming, incident response) with **soft skills** (communication, problem-solving, teamwork). Common certifications like **Security+**, **CISSP**, and **OSCP** also appear frequently, along with knowledge of **risk management frameworks (RMF, NIST, DoD standards)**.

Top 10 Most Popular Cybersecurity Skills & How Students Can Master Them

1. **Networking & Network Security (LAN, WAN, Firewalls, VPNs, IDS/IPS)**
 - *How to master:* Take Cisco's **CCNA** certification courses, set up virtual labs using Cisco Packet Tracer or GNS3, and practice configuring routers/firewalls.
2. **Risk Management & Compliance (RMF, NIST, DoD STIGs, HIPAA, GDPR)**
 - *How to master:* Study NIST Cybersecurity Framework and pursue **CompTIA Security+** or **CISA** certifications. Join campus cyber policy groups or compliance projects.

3. **Operating Systems & System Administration (Linux, Windows, Active Directory)**

- *How to master:* Install and manage Linux/Windows servers in virtual machines, take Microsoft or Linux Foundation courses, and pursue **Linux+** or **Microsoft Azure certs**.

4. **Cloud Security (AWS, Azure, GCP)**

- *How to master:* Enroll in **AWS Certified Security Specialty** or Microsoft Azure security certification. Use student free credits to practice cloud labs.

5. **Programming & Scripting (Python, Bash, PowerShell, Java)**

- *How to master:* Take Python for Cybersecurity courses, practice scripting for automation, and build projects like log analyzers or vulnerability scanners.

6. **Incident Response & Forensics (SIEM tools, malware analysis, digital forensics)**

- *How to master:* Practice with tools like **Splunk**, **Wireshark**, **Autopsy**, or **Volatility**. Join cyber competitions (e.g., CTFs) that include forensics challenges.

7. **Penetration Testing & Ethical Hacking (OSCP, Kali Linux, Metasploit)**

- *How to master:* Use **Hack The Box**, **TryHackMe**, or **OverTheWire** platforms. Work toward **OSCP** or **CEH** certifications.

8. **Cryptography & Secure Protocols (PKI, SSL/TLS, Encryption Standards)**

- *How to master:* Take a cybersecurity cryptography course, build small projects using OpenSSL, and study applied crypto in real-world systems.

9. **Security Tools & Frameworks (SIEM, HBSS, ACAS, Splunk, RedSeal, McAfee SIEM)**

- *How to master:* Download community editions of SIEM tools, take Splunk Fundamentals training, and practice analyzing logs.

10. **Soft Skills (Communication, Problem-Solving, Teamwork)**

- *How to master:* Join cybersecurity clubs, present projects, write security reports, and participate in team-based competitions like **CyberPatriot** or **NCL**.
-

✅ These 10 areas cover the **core mix of technical, analytical, and communication skills** that show up repeatedly in the jobs listed in your spreadsheet.

Would you like me to **map specific jobs in the spreadsheet to these skills** (e.g., “Penetration Tester → Pen Testing & Scripting”)? That way you’ll see exactly how each role emphasizes different skills.

Sources: ChatGPT