Akon Deng

Cybersecurity Analyst: Mixing Human Skills and Tech

Intro

In today's online world, cybersecurity professionals do more than just tweak firewalls and update software. A cybersecurity analyst is basically the detective and teacher of the online world. They scan networks daily for weird activity, flag suspicious traffic, and attempt to stop things from happening whenever a security breach happens. But what people don't realize is that they also lean heavily on social science. Like knowing how people think, communicate. Also, forming habits helps analysts build stronger defenses and connections with real users.

Why Social Science Matters

Cyber analysts study psychology to see how fear, trust, and urgency push people to click bad links. They look at which words like urgent or official trigger a panic response, then share these findings with coworkers so everyone can understand the threat.

Beyond psychology, analysts also borrow from sociology and anthropology to see how different groups use technology. For example, a college student might use campus Wi-Fi 24/7, while an older neighbor only hops online to FaceTime with grandkids. By observing these patterns, analysts create training sessions that feel less like boring lectures and more like helpful conversations.

Working with Different Communities

Not everyone has a high-end laptop or a VPN subscription. Groups such as low-income families, immigrants learning English, or older adults often lack digital safety. Cyber analysts plan hands-on workshops in community centers, translate checklists into multiple languages, and use real-life examples like how to spot a fake bank email instead of screens full of code.

When analysts do ethical hacking or digital forensics, they handle sensitive data from diverse people. Ethics taught in social science courses warns people to avoid bias and never assume that one group causes more problems, and to respect everyone's privacy. If a small nonprofit is hacked, analysts treat the staff and clients with empathy, remembering these are people's livelihoods and not just case studies.

Putting Class Ideas to Work

During class I covered concepts like socialization, inequality, and power dynamics—all super relevant in cybersecurity. Like inequality: big tech companies might roll out security updates that only work on the latest devices, leaving smaller organizations exposed. Analysts can gather research showing the gap between them, then pitch more inclusive solutions to managers. That's using power dynamics theory to influence policies.

Communication was another class discussion. Writing a breach report for your boss requires a formal tone and data charts. Explaining the same breach to non-tech staff

calls for metaphors—think of your password like a house key—and a friendlier style. Analysts adjust their language based on who's listening just like practiced.

Conclusion

Being a cybersecurity analyst isn't just all about code, servers, or different security protocols. It's just as much about people—understanding how they behave, learning what things they may need, and translating technical language into clear advice. By blending social science—psychology, sociology, and ethics—with technical know-how, analysts can protect people from big corporations down to the most vulnerable neighborhoods. As cyber threats keep evolving daily, the analysts who master both the human side and the technical side will be the ones keeping the digital world safe and easier to use.