Nigel Adkins
February 25
CYSE 200T
Professor Duvall

Julia Nickel FBI three things that resonated with me

BLUF:

1 FBI is intelligence and law enforcement. They only deal with Federal crimes, CISA = protection and the FBI responds to the bad things that happen. Companies come to the FBI as a victim and work with them to get the bad guys through intelligence sharing with a company or with the public.

2 Cyber threat actors: Nation state cyber threat actors, someone that's conducting nefarious activity on behalf of another government, China, Iran, North Korea, and Russia are some of the most common, through crypto, manufacturing, energy, and many more ways. China is the most active and persistent threat to the private sector of the U.S.. Russia tends to target a lot of defence and technology sectors. Iran goes after critical infrastructure. North Korea goes after defence and nuclear activities.

3 what they do: Reconnaissance, they do research before targeting the network, then co promise like phishing, then foothold to get in the network, escalate privileges, Move laterally, expand presence, exfiltrate data, and maintain presence.

4 How they do it: cheapest and fastest methods, exploitation of trust and connections, zero day exploits, live off the land, exploitation of publicly available tools and information.

5 Cyber criminal threat: they do it for the money, many methods and techniques used. Global,

FBIjobs.gov

Collegiate hiring program