1. Summarize how cybersecurity threat landscape evolved in 2020.
   Due to covid-19, naturally there has been a drastic rise of working from home. Some threats that were faced by companies during 2019 will now be magnifying throughout 2020. These threats area as follows:
    a. Ransomware: With creations like WannaCry and NotPetya, ransomware and been gaining a steady popularity and now is thought as one of the greatest threats facing a business. For 2020, variants like Ryuk and Sodinokibi target large enterprise with demands shooting upwards of a million dollars. As in 2019, there would be improvements and evolutions in the ransomware in 2020 as well.
    b. Phishing: Due to the panic and the climate of uncertainty moving widely during the early years of 2020, the effectiveness of phishing attacks rose. To further the improvement and efficiency of phishing, AI and ML are being used. The effectiveness of phishing emails and landing pages will be automatically tested to improve conversion rates, and common maintenance activities, like registration of new phishing domains, may become increasingly automated.
    c. Credential Stuffing: Malicious bots comprise $1/5^{th}$ of the internet traffic. Due to covid-19, companies are exposing more systems to the public internet, via VPN, to enable employees work effectively from home. This brings in more accounts to being exposed to cybercriminals allowing credential stuffing to take place widely.
    d. Cloud Breach: Each year, tons of data gets added to the cloud, 2020 isnt any different. Despite of the lockdown in several countries, data is still uploaded in the cloud. In 2020, more sensitive data is added to cloud deployments, the rate and the volume of cloud data breaches is only expected to increase. Due to the increase of credential stuffing, cloud breaching get that much more likely to happen. One popular example is the hack on RedEngine and CDPR games. The impact of this breach made news worldwide. This negatively affected the company in drastic ways. Like updating the release calendar of games and coming up with different projects. Even locating back the stolen code is currently an on-going process.
    e. IOT/ IOMT- Focused Attacks: Covid-19 has made health care a massive target in several domains. Cybersecurity, without doubt is one of them. During this year, IoT devices may be capable of viewing computer screen containing sensitive patient and company data. This can comprise recorded video and voice calls as well, thus triggering a mass hysteria.
    f. Cybersecurity skills Gap: With lack of guidance and physical gap in 2020, due to covid-19, practically knowledge and skills have been put to a pause. Globally, the cybersecurity force must be growing 147% to meet the demand. Due to 2020, it is likely that there is going to be a greater percentage need.
2. What is credential stuffing attack?

Is the automated injection of breached username/password pairs in order fraudulently gain access to user accounts. It is a new form of attack that accomplishes account takeover through automated web injections. Since 62% of the people reuse passwords across personal and business accounts, breached passwords present a significant threat to enterprise security.