**The SolarWinds CyberAttack**

* **Give an overview of what the breach was and the motivations behind it.**
* The SolarWinds CyberAttack was a breach in the supply chain involving the SolarWinds Orion system. In this cyberattack, hackers now identified as Nobelium by Microsoft “gained access to the networks, systems and data of thousands of SolarWinds customers,” according to Tech Target. The article details that “More than 30,000 public and private organizations -- including local, state and federal agencies -- use the Orion network management system to manage their IT resources.” Consequentially, a horrifying amount of sensitive data fell into the wrong hands with the SolarWinds cyberattack. As for the motivation of the attack, the article details that SolarWinds “privileged position and its wide deployment,” particularly in terms of its “access to IT systems to obtain log and system performance data” made it a “lucrative and attractive target.”
* **Explain where the “tech flaws” were, and how hackers were able to breach their system.**
* In the SolarWinds cyberattack, the hackers employed a supply chain attack, which Tech Target defines as an attack that “works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.” In the SolarWinds cyberattack, the third party software was the SolarWinds Orion system. According to Slate, “Orion’s software, it turned out, was protected by a very flimsy password (“[solarwinds123](https://www.reuters.com/article/global-cyber-solarwinds-idUSKBN28P2N8)”).” Consequentially, when users clicked on a new SolarWinds software update, they downloaded malware. Tech Target explains that SolarWinds was a perfect target for [this kind of supply chain attack](https://www.techtarget.com/searchsecurity/news/252493761/SolarWinds-breach-highlights-dangers-of-supply-chain-attacks).” Furthermore, “Because their Orion software is used by many multinational companies and government agencies, all the hackers had to do was install the malicious code into a new batch of software distributed by SolarWinds as an update or patch.” In terms of the effects of this attack, Tech Target further explains that “The third-party software, in this case the SolarWinds Orion Platform, creates a backdoor through which hackers can access and impersonate users and accounts of victim organizations. The malware could also access system files and blend in with legitimate SolarWinds activity without detection, even by antivirus software.”
* **What has the company done to protect against that vulnerability since?**
* In the aftermath of the SolarWinds cyberattack, Solarwinds sought to have its customers update their Orion platforms. Specifically, according to Tech Target, “The company has released [patches for the malware and other potential vulnerabilities](https://www.computerweekly.com/news/252495701/SolarWinds-patches-two-critical-CVEs-in-Orion-platform) discovered since the initial Orion attack.” Also, SolarWinds “recommended customers not able to update Orion isolate SolarWinds servers and/or change passwords for accounts that have access to those servers.”