Great post on mentioning the different layers for protecting an organization. While VPN is supposed to offer protection, vendors are key to ensuring that appliances are kept in check to ensure company security. If we look at the recent attacks on FortiGate for example, a flaw in the firmware allowed hackers to expose thousands of credentials and this leads to companies not knowing if they have been hacked and what information has been stolen. Companies need to go out of their way to patch the operating system of the devices, change every single password in the organization that connects to VPN and should look at implementing additional layers like multi-factor authentication on accounts (Charlie Osborne, 2021).

I agree that companies should invest in solutions like SOAR (Security Orchestration Automation and Response) because this can detect a potential attack and allow them to mitigate it before it is too late.

According to research, it takes companies on average “228 Days” to identify a breach (Rob Sobers, 2021). This just shows that companies are not tuned it to what happens in the background or what is going on in the environment. Investment in Cybersecurity should be the top priority and focus of the IT division. If the IT division is outsourced, they need to look at partners that will assist them on the road to securing their environment, which includes performing an inventory of patch levels, not only on the external devices like Routers, Switches and other networking equipment but also the software and operating systems running on users’ machines.

References

Charlie Osborne. (2021) Attacker releases credentials for 87,000 Fortigate SSL VPN devices. Available From: <https://www.zdnet.com/article/attacker-releases-credentials-for-87000-fortigate-ssl-vpn-devices> [Accessed 21 September 2021].

Rob Sobers. (2021) 98 Must-Know Data Breach Statistics for 2021. Available From: <https://www.zdnet.com/article/attacker-releases-credentials-for-87000-fortigate-ssl-vpn-devices> [Accessed 21 September 2021].