Sock Co. Onboarding Letter

Department: Security Operation Center

Position: Lead Security Engineer

Hello, *Employee #196,* and welcome to Sock Co!

We are happy to have you as part of the team at the world's largest e-commerce Sock company, Sock Co! My name is Ted, and I will be helping you with the onboarding process. We will not sugar coat it; you have some serious work to do. Hours will be daunting, and at times, it may feel like you are living in a sock, or in your case, a SOC. (We are fun, we have fun here.) I would like to best prepare you for what is to come, as we have had a lot of turn over with personnel in the SOC due to a very demanding workload. I will admit, a lot of the stress was self-induced due to falling to obvious phishing emails. Our employees do not seem to understand the importance of not clicking links in emails!

You will oversee our overall security structure for the company, and report to your terribly busy CISO as he will have no time to make decisions; that will be on you! We are a small 100–200-person company with an on-prem active directory infrastructure. (We are 100% on-prem, no cloud infrastructure in our environment.) All employees are assigned a Windows 10 Laptop which is domain joined by our IT department. We also have a plethora of Linux Servers hosting our web infrastructure to, you guessed it, sell socks!

Let's talk about security products. Endpoint monitoring is in a rough state at the moment. We are currently checking out several vendors for the best price and security coverage. The Security engineers on the team are not remarkably familiar with Endpoint Policy configurations. They will need training for file integrity and process monitoring, so we need a user-friendly EDR (Endpoint Detection and Response) product with extensive training to get secure as fast as possible. We also understand that most Endpoint products allow the creation of custom-made detections. This is something we do not currently have and would love to build our own library of detections eventually. As for Network security, we are very well versed as we need to ensure that our web traffic is secure. We have several security controls for network protection such as web proxies, web content filters, and NextGen Firewalls which have excellent policy configurations that already have shown to detect and prevent malicious traffic with a low false positive rate. We currently utilize Splunk as our log aggregation and correlation engine for network events, and we plan to implement EDR products once we have decided which ones to go with.

Our IT team is new with not a whole lot of security experience. They are familiar with Windows infrastructure but may need your help with access control settings so we can ensure that users have least privileged access.

We are happy to have you! Now please, secure our company!