1. Hi everyone, here is an overview of the security measures in place on corporate applications.
2. The corporate applications are split in 2 parts with a frontend and backend. The way that they communicate with each other is through an API that allows user requests to be taken and information gathered to deliver the info.
3. The application layer API plays a key role in communication between the user interface and the backend.  The API takes in ACL groups and roles to display the applications that the users are allowed to access using a dashboard and menu. APIs are designed to by business requirements and dictates what   applications are shown on the dashboard to a user.
4. Another security measure on our applications Is that logging and monitoring happens on all activity for an application. The logs are centralized in sumo logic where it can be flagged for malicious activity and investigated by infosec.
5. security is considered from the start of development. An application is developed in 4 stages, dev, test, staging and production. Each step tests the functionality of the code as well as its effect on other components in the application. For each stage, we use Jenkins to run a deployment pipeline that makes sure the code is compliant with business requirements. Within the pipeline, 3 security scans on done using Veracode, Sonarqube and Quality gateway to ensure secure coding and mitigate vulnerabilities from happening.