Scenario Background

Kelvin Control Enhancements Ltd (KCE) is a company that provides specialist services to a local nuclear power station. Originally, KCE provided safety-critical Operational Technology (OT) including sensors, controllers and monitoring capability, but then expanded to include the provision of Field Engineers. One of its recently added services is a complex HR function called MindfulCheck that monitors and analyses the physical and mental well-being of workers in dangerous and high stress roles.

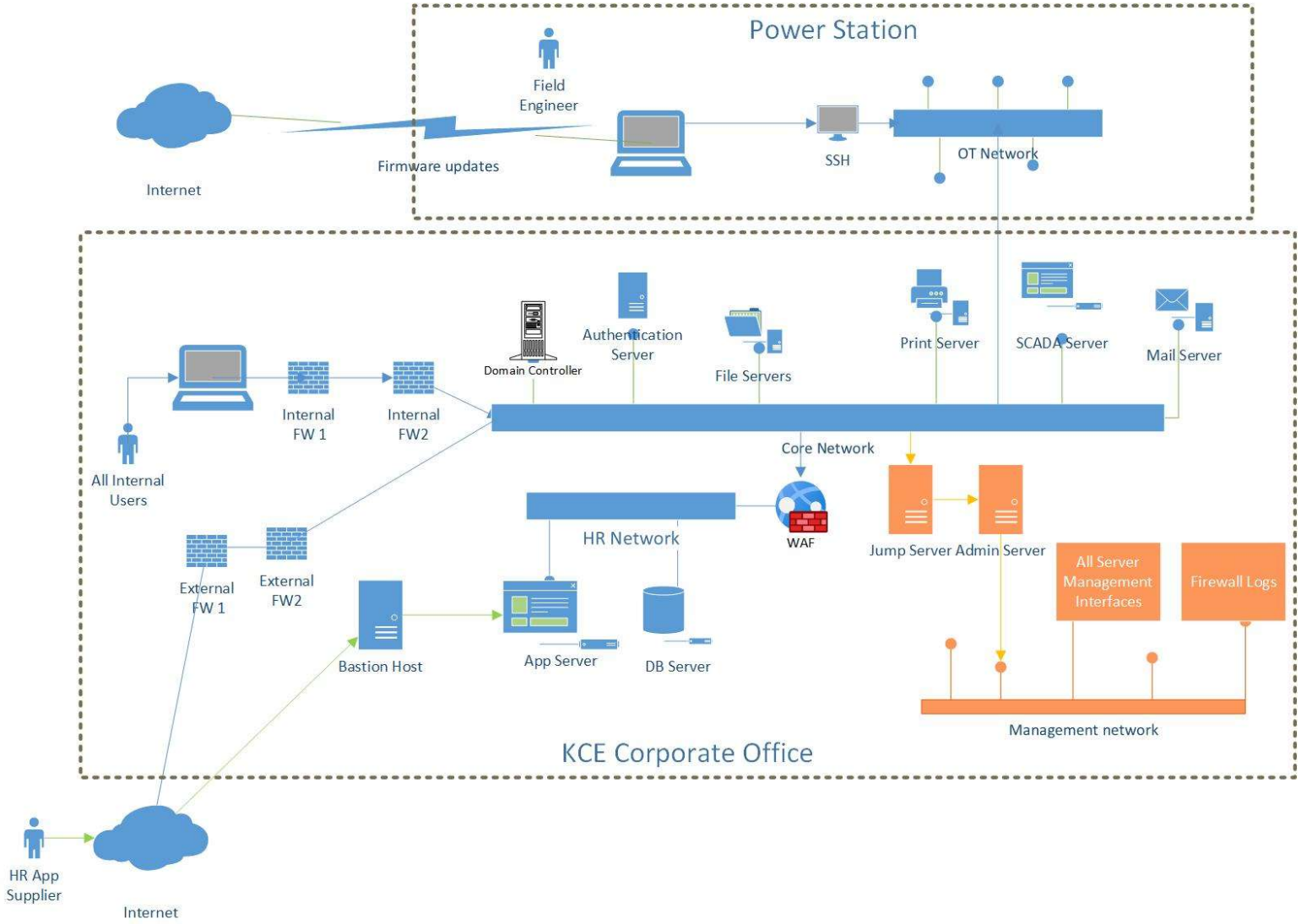
Another recent service provision allows KCE to use Supervisory Control and Data Acquisition (SCADA) technology to remotely manage and control of some of the power stations OT from KCEs corporate office, in addition to the Field Engineers who are onsite at the power station. Field Engineers (sometimes subcontractors) in and around the power station use KCE Laptops to login to the Modbus Network that connects the Industrial Control System (ICS) devices. Firmware updates for OT devices are downloaded onto the laptops from vendor websites through the Internet. KCE operators in the Corporate Offices can log in to the core KCE IT network to use monitoring and control software which connects to the OT devices on the OT network.

KCE MindfulCheck specialists also login to the KCE IT network. They then login to the app from their browsers via a Web Application Firewall (WAF). The MindfulCheck Supplier was originally given access to install, configure and bug check the HR Application. They have retained this access to conduct annual patching, updates and other checks using PowerShell.

All KCE staff – mostly permanent but sometimes temporary agency admin staff - log in to the Core IT Network in its commercial office. Users who are given Admin duties can connect to the Admin Server via a "jump server" bastion host to access the management network. The management network is a physically separate network that accesses all server management interfaces and event logs collected from the firewalls.

A recent audit by client security specialists has criticised KCE's security, but this document is not available to you. There have been rumours that KCE information has appeared on the Internet. There have been complaints from clients that personal information has leaked from MindfulCheck and that it is often inaccurate, with important information possibly tampered with or deleted. In addition, KCE accidentally deleted a large quantity of financial records which is causing it considerable tax difficulties – it has not been able to recover the data.

Below is a diagram of the KCE systems hastily drawn up by the IT Manager. It is therefore far from comprehensive and designed to give only a brief introduction:



Your Account Manager has had an initial sales meeting with the company - the background information above was sent by the KCE IT Manager who appears to be the only contact interested in security. The main impetus at the sales meeting came from the Operations Director and Finance Director, who bullied the IT Manager somewhat. Your colleague took the following notes based on the Directors' comments:

"We don't really have a security policy or standards. We just let the IT manager get on with it. As long as he stays in budget, we're OK."

"We can't patch the Operational Technology Network due to our contracted Key Performance Indicators and safety cases requiring 24/7 access to the monitoring service. Is that a security problem or an operations problem?"

"To save money, the company is considering allowing BYOD for the field engineers. What are the potential implications and how could we ensure zero security impact?"

"Don't know what the Admin guys do all day except eat pizza. What actually are the most important activities that the Admin team should be carrying out?"

"Someone said we should be using longer passwords - that sounds like a dumb idea. What do you think?"

"We think there may have been a data leak, but the IT team say that the logs don't show any attempts at unauthorised or unauthenticated access to that data. What might have happened? Can we go back and check? Why do people keep talking about passing hash?"

"We'd like to get this all on Cloud. The IT manager has designed a Cloud implementation that perfectly follows our current system design and server laydown - to be dropped on top of an Infrastructure-as-a-Service public cloud. What would you advise?"

"We have a high turnover of Field Engineers - they're always putting their CVs online telling everyone what brilliant work they do at the power station."