Endpoint Protection Planning and Integration

The purpose of this lecture is really twofold.

- First there is Planning - With what you will learn in this lecture you should be able to develop an effective security installation plan for your organization.
- Then we have integration - In this lecture we will gain an understanding of how these individual components integrate together to form a solid security solution.

The following is a summary of the individual components and a brief explanation of the function of each major component. If you have setup your lab as prescribed in previous lectures, all those components marked as completed should already have been installed and configured in your lab.

For this lecture, the following components should be installed in the order given below.

Installation of Windows server, Active Directory, DNS, SQL, SCCM and Endpoint Protection should have been completed.

Endpoint Protection – Should already be installed if you downloaded and installed SCCM with Endpoint Protection.

- **WSUS server role** must be installed, In this case on ITFSCCM01.

- Installation of the **Software Update Point Role** – This role runs the Windows Software Update Services (WSUS) and allows Configuration Manager to use the WSUS catalog to scan SCCM clients for software updates. The SUP is the connection between WSUS and SCCM. For this lecture, the SUP enables us to bring software updates into SCCM.

- SCCM uses DNS and Active Directory to find users and devices so we can create collections for software and policy deployment.

- Installing the **Reporting Services Point Role**– A site service role that provides integration with SQL server reporting services to create and manage reports for Configuration Manager.

- Installing the **Endpoint Protection Point Role** – Must be installed on one site system server at the top of the hierarchy.

So far we have planned our server side configuration, now we will plan our **client side configuration**

- **Configure Custom Client Settings –** This procedure configures Custom client settings for Endpoint Protection, which can be deployed to collections of computers in your hierarchy.

- Deploy the default or a custom **Antimalware policy**. This can be deployed to all devices or to your choice of device collections.
- From within each antimalware policy you can configure scheduled scans. You can remove malware, and you can use the reporting functionality of SQL to send warnings and alerts to SCCM or automatically send yourself an email concerning malware infection.

- **Configure a Firewall Policy** – This allows you to perform basic Windows Firewall configuration and maintenance tasks on the client computers in your hierarchy, for greater control with more options use group policy.

- Creating an **Automatic Deployment Rule**. You can automatically approve and deploy software updates by using an automatic deployment rule.
  This rule defines what updates will be downloaded for various products, for this lecture we chose to download windows defender updates there are many other products listed.

You can set the source to define the order in which to receive definition updates. You can set your location to where these updates will be stored before they are pushed out.

- **Deploy Windows 10 Clients** – Windows 8 and earlier required the Endpoint Protection client installed to the Windows computer. With Windows 10, Windows Defender is the default Windows 10 Antimalware client, so you don't need to install another client, but in effect what you need to install is a management layer so that the client can be managed by configuration manager.

Congratulations you have completed this lecture, thanks for watching, and we will see you in the next lecture