Filename: microsoft-ms101-6-4-1-configure-microsoft-365-atp-policies
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: Configure Microsoft 365 ATP Policies
Description: Adam and Wes discuss how to configure Microsoft 365 ATP Policies.

Configure Microsoft 365 ATP Policies

Implement Microsoft 365 Security and Threat Management (30-35%)

Implement Threat Management
• Plan a Threat Management Solution
• Design Azure Advanced Threat Protection (ATP) Policies
• Design Microsoft 365 ATP Policies
• Configure Azure ATP Policies
• Configure Microsoft 365 ATP Policies
• Monitor Advanced Threat Analytics (ATA) incidents

==========

Configure Microsoft 365 ATP Policies

Things to know for the exam

Anti-Phishing:

```
1. Look at the ATTACK SIMULATOR TOOLSET (available with E5) and understand
```

what it is used for & how it helps to identify phishing vulnerabilities

```
What is a Spear Phishing Attack - designed to harvest credentials by tricking
```

people into clicking on links or divulging information

```
What is a Brute Force Password Attack - targeted at a single user, using
```

multiple attempts to guess their password from a pre-configured list of
possible password choices

```
What is a Password Spray Attack - targeted at multiple users, using the same
```

single password against them all

```
2. Look at the EXPLORER TOOLSET

3. Look at the REVIEW TOOLSET
```

Know the permissions

To view reports:

```
Organization Management Role
Security Administrator Role
Security Reader Role
```

Organization Management can control permissions for others and configure
everything

Security Reader is a read-only view of the o365 Security & Compliance Center

Anti-Spam:

```
1. Enabled by default
2. Changes can take up to 1 hour to propagate
3. Use the MESSAGE TRACE TOOL (MAIL FLOW) to figure out if a message was
```

dropped due to being identified as spam

Anti-Malware:

```
1. STANDALONE CUSTOMERS - most email messages are scanned, BUT NOT ALL !!! -
```

Messages sent between internal recipients ARE NOT SCANNED

```
2. Enterprise Plan Customers - ALL EMAIL IS SCANNED !!!

3. Remember the MESSAGE TRACE TOOL

4. Remember PowerShell can be used to manage anti-malware policy

    Get-MalwareFilterPolicy
    Set-MalwareFilterPolicy
    New-MalwareFilterpolicy
    Remove-MalwareFilterPolicy

5. You can use the EICAR.TXT file to test anti-malware functionality
```