Filename: microsoft-ms101-6-1-4-ata-architecture-and-components
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: ATA Architecture and Components
Description: Adam and Wes discuss the architecture and components of the ATA solution.

ATA Architecture and Components

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

==========

ATA Architecture and Components

ATA consists of the following components:

```
• ATA Center - receives data from any ATA Gateways and/or ATA Lightweight
```

Gateways you deploy.

```
• ATA Gateway - installed on a dedicated server that monitors the traffic from
```

your domain controllers using either port mirroring or a network TAP.

```
• ATA Lightweight Gateway - installed directly on your domain controllers and
```

monitors their traffic directly, without the need for a dedicated server or configuration of port mirroring.

An ATA deployment can consist of a single ATA Center connected to all ATA Gateways, all ATA Lightweight Gateways, or a combination of ATA Gateways and ATA Lightweight Gateways.

To enhance ATA detection of Pass-the-Hash, Brute Force, Modification to sensitive groups and Honey Tokens, ATA needs the following Windows events:

```
• 4776
• 4732
• 4733
• 4728
• 4729
• 4756
• 4757
```

These can either be read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight Gateway is not deployed, it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEM events or by Configuring Windows Event Forwarding.

ATA prerequisites:

The ATA System works on active directory forest boundary and supports Forest Functional Level (FFL) of Windows 2003 and above.

Do not install Microsoft Message Analyzer on an ATA Gateway or Lightweight Gateway. The Message Analyzer driver conflicts with the ATA Gateway and Lightweight Gateway drivers. If you run Wireshark on ATA Gateway, you will need to restart the Microsoft Advanced Threat Analytics Gateway Service after you have stopped the Wireshark capture. If not, the Gateway stops capturing traffic. Running Wireshark on an ATA Lightweight Gateway does not interfere with the ATA Lightweight Gateway.

https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites