Filename: microsoft-ms101-6-1-1-plan-a-threat-management-solution
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: Plan a Threat Management Solution
Description: Adam and Wes discuss what steps need to be taken to successfully plan a Threat Management solution.

Plan a Threat Management Solution

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

==========

Plan a Threat Management Solution

What is Azure Advanced Threat Protection (ATP)? (CLOUD)

A cloud-based threat protection solution that is focused on users and their behavior.

Products that are part of ATP:

```
• Azure ATP
• Windows Defender ATP
• Office 365 ATP
```

What is Advanced Threat Analysis (ATA)? (ON-PREM)

An On-Premise solution that analyzes network traffic and learns how your users behave.

This information is collected by ATA via:

```
• Port mirroring from Domain Controllers and DNS servers to the ATA Gateway and/or

• Deploying an ATA Lightweight Gateway (LGW) directly on Domain Controllers
```

ATA can receive events and logs from:

```
• SIEM Integration
• Windows Event Forwarding (WEF)
• Directly from the Windows Event Collector (for the Lightweight Gateway)
```

Key integration and technologies to be aware of for the exam:

```
• Azure Security Center - ATA integrates with Azure Security Center allowing
```

you to review and interact with your alerts

```
• Windows Defender ATP - Can integrate with Azure ATP to provide more
```

complete coverage of the organization's devices; Azure ATP for servers and Windows ATP for client devices

```
• VPN - Both Azure ATP and ATA can integrate with VPNs. RADIUS accounting
```

events are forwarded to both Azure ATP and ATA.

For Azure ATP, UDP port 1813 INBOUND must be opened to the server(s) where the sensors are located.

For ATA, UDP port 1813 INBOUND must be opened to the ATA GATEWAY (SERVER) or ATA LIGHTWEIGHT GATEWAY (Domain Controller).

```
• SIEM/Syslog - Azure ATP can send notifications to SIEM/Syslog servers


NOTE: (OLD INFO, BUT MAY STILL BE ASKED ABOUT FOR EXAM AS OF JULY/AUGUST 2019)

You must download and install an agent to integrate ATA with Azure Security
Center. During the integration, a download link is provided. You also need to
have a Log Analytics Workspace in Azure.


NOTE: (NEW INFO, WILL BE ASKED ABOUT AT SOME POINT FOR EXAM !!!)

Azure Sentinel is now the Cloud based/Azure Integrated SIEM solution that
ties this all together along with the Security Center.

Azure Sentinel aggregates data from all sources, including users, applications,
servers, and devices running on-premises or in any cloud. It includes built-in
connectors for easy onboarding of popular security solutions. Collect data from
any source with support for open standard formats like CEF and Syslog.
```