Filename: microsoft-ms101-6-5-1-monitor-advanced-threat-analytics-incidents
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: Monitor Advanced Threat Analytics (ATA) Incidents
Description: Adam and Wes discuss how to monitor Advanced Threat Analytics (ATA) incidents.

Monitor Advanced Threat Analytics (ATA) Incidents

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

==========

Monitor Advanced Threat Analytics (ATA) Incidents

Read through the document and DO NOT MEMORIZE !!!, however, be familiar with capabilities, limitations and remediation options. Focus on:

```
• Changes to sensitive groups
• Brute-Force Attacks
• Pass-the-hash Attacks
• Pass-the-ticket Attacks
• Remote Execution Attempts
```

Advanced Threat Analytics suspicious activity guide:
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide

The ways that ATA provides information:

```
• Alerts
• Suspicious activities time-line
• Notifications
• Reports
    • Summary Report
    • Modification of Sensitive Groups
    • Password Exposed in Cleartext
    • Lateral Movement Path to Sensitive Accounts
```

Remember that ATA gathers information from Domain Controllers. You can add additional sources:

```
• Configure Windows Event Forwarding
• Configure VPN Integration
• Tag Sensitive Accounts (beyond the default ones already tagged)
```

Event IDs to enhance ATA Capabilities:

```
|========|=======================================================|
| 4776 | DC authenticates a user by using NTLM |
|========|=======================================================|
| 4732 | Group membership addition for Domain Local Group |
|========|=======================================================|
| 4733 | Group membership removal for Domain Local Group |
|========|=======================================================|
| 4728 | Group membership addition for Global Group |
|========|=======================================================|
| 4729 | Group membership removal for Global Group |
|========|=======================================================|
| 4756 | Group membership addition for Universal Group |
|========|=======================================================|
| 4757 | Group membership removal for Universal Group |
|========|=======================================================|
| 7045 | A new service was installed/added |
|========|=======================================================|
```

Three sections in the ATA Portal to allow you to review information on demand:

```
1. Timeline
2. Reports
3. Health
```