Microsoft

Microsoft Security Operations Analyst

Exam Ref SC-200

Yuri Diogenes
Jake Mowrer
Sarah Young

Microsoft

Exam Ref SC-200 Microsoft Security Operations Analyst

Yuri Diogenes
Jake Mowrer
Sarah Young

Threat and Vulnerability Management (TVM) in Microsoft Defender for Endpoint does not have these issues for the following reasons:

1. **There is no agent** The sensor is built into the Windows Operating System.
2. **There is no scanning** The Defender for Endpoint service that reports EDR data also reports these weaknesses and vulnerabilities on an ongoing basis.
3. **No corporate network required** Any time the device has access to the Internet, it can send data since the Defender for Endpoint service is in Azure.
4. **Vulnerabilities and configuration weaknesses are prioritized based on risk to the organization** When the risk of a vulnerability or configuration weakness raises, such as when a public exploit is posted that uses a vulnerability, the prioritization dynamically changes to ensure that you remediate the riskiest vulnerabilities and weaknesses in your environment.

MORE INFO **THREAT AND VULNERABILITY MANAGEMENT**

For more information about threat and vulnerability management, see *https://aka.ms/sc200_tvm*.

Threat & Vulnerability Dashboard

You need to have a quick and clear view of the weaknesses and vulnerabilities that are present across your organization. The Threat & Vulnerability Dashboard is a great way to get this comprehensive, high-level assessment. Follow these steps to familiarize yourself with the dashboard.

1. Log in to *https://security.microsoft.com* as a member of the **Global Administrator** or **Security Administrator** Azure Active Directory roles or as a member of an Endpoint role with the **View Data—Threat And Vulnerability Management** permission.
2. Under **Endpoints**, expand **Vulnerability Management** and click **Dashboard**.
3. The following tiles are shown in the dashboard shown in Figure 1-95.
   - **Exposure Score** This shows the amount of exposure affecting devices in your organization. Ideally, you want the score to be as low as possible.
   - **Top Security Recommendations** This is a list of actions you can take to lower your Exposure Score. They are ordered by **Impact**, which is the measure of the number of points by which your Exposure Score will be lowered by remediating that action
   - **Microsoft Secure Score For Devices** This rates the security posture of your environment based on **Application, OS, Network, Accounts,** and **Security Controls**. A higher percentage indicates a better security posture.
   - **Exposure Distribution** This shows the number of devices that are susceptible to attacks, which are ranked as **High, Medium,** and **Low**.

- **Remediation Activities** This is a list of activities to remediate vulnerabilities and configuration weaknesses.
- **Top Vulnerable Software** This is a list of software with vulnerabilities that is intelligently ranked on factors such as number of vulnerabilities, threats, and number of affected devices.
- **Top Exposed Devices** This is a list of devices with the most exposure that is intelligently ranked on factors such as number of vulnerabilities, threats, and security recommendations.

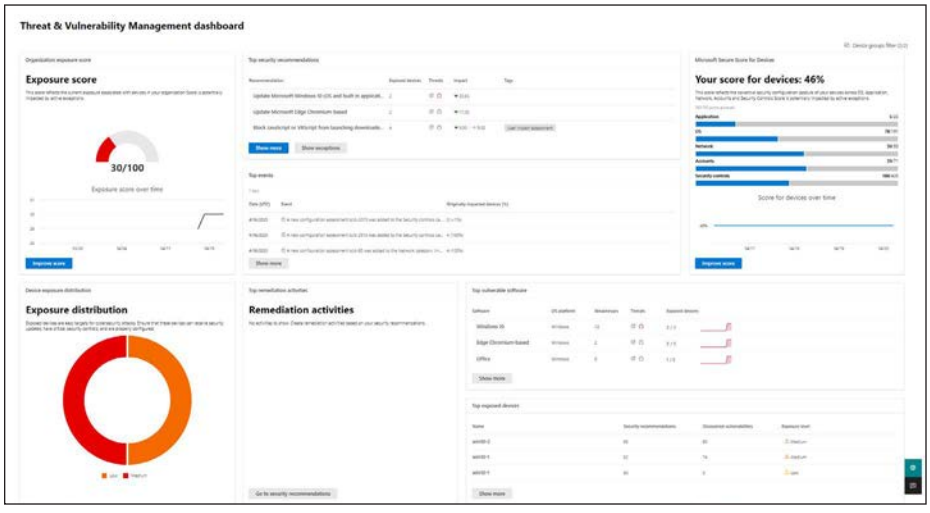

FIGURE 1-95 Threat & Vulnerability Management Dashboard

Remediation activities and exceptions

Now that you have your security recommendations ranked intelligently and dynamically, you need to assign remediation activities to the individual or teams responsible for patch management. The Threat & Vulnerability Management Dashboard tells you which actions to take first that will have the **greatest impact in lowering the risk** in your environment.

EXAM TIP

Be sure to know how to create a remediation activity and exceptions!

Follow these steps to create a remediation activity:

1. Log in to *https://security.microsoft.com* as a member of the **Global Administrator** or **Security Administrator** Azure Active Directory roles or as a member of an Endpoint role with the **Active Remediation Actions: Threat And Vulnerability Management—Exception Handling And Remediation Handling** role.

2. Under **Endpoints**, expand **Vulnerability Management** and click **Recommendations** to open the view shown in Figure 1-96.

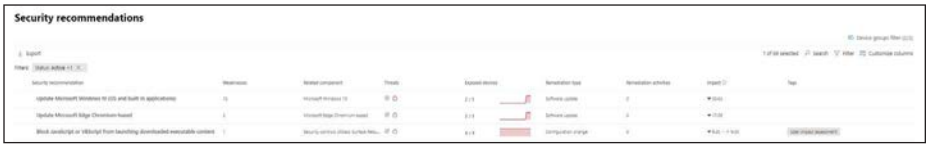

FIGURE 1-96 Security recommendations

3. Just remediating the **Update Microsoft 10 (OS And Built-In Applications)** line item will result in the Exposure Score lowering by 30.65 points. One of the reasons this action will lower the score is because there is a verified, public exploit available for some of the vulnerabilities that these two devices are affected by.
4. You can tell if there is an exploit available for one or more of these vulnerabilities by looking at the icons under **Threats**. These threats indicate the following:
   - **Threat insights** As shown in Figure 1-97, when this icon is red, there is a publicly available exploit for one or more vulnerabilities.

FIGURE 1-97 Threat insights icon

   - **Breach insights** If this icon is red, there is an active alert attributed to the vulnerability, as shown in Figure 1-98.

FIGURE 1-98 Breach insights icon

5. Click **Update Microsoft Windows 10 (OS And Built-In Applications)** in the list of security recommendations.

6. Click **Request Remediation** to open the view shown in Figure 1-99.

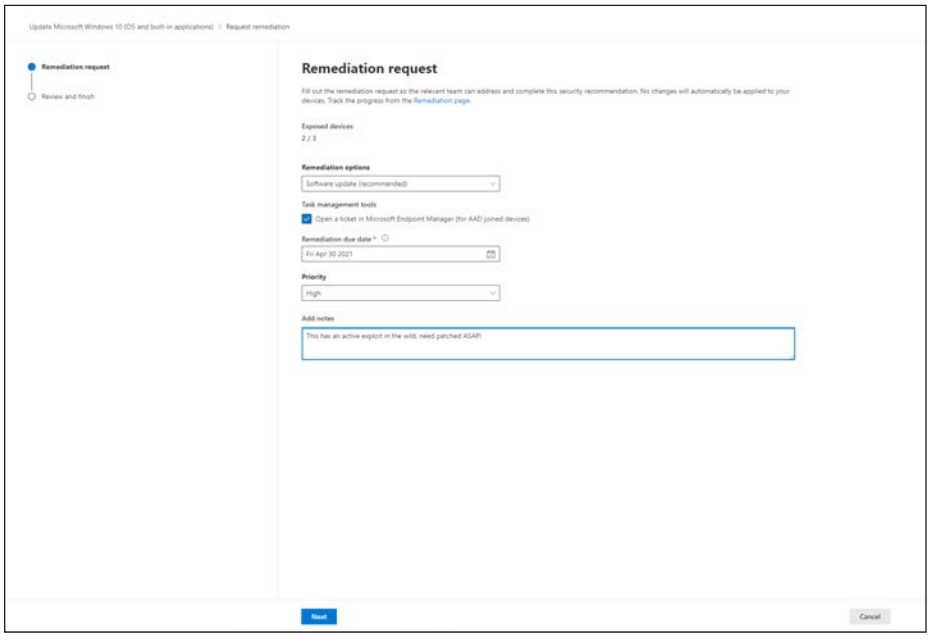

FIGURE 1-99 Remediation Request wizard

7. Select **Software Update (Recommended)** under **Remediation Options**.
8. Select the **Open A Ticket In Microsoft Endpoint Manager (For AAD Joined Devices)** check box.

> ***TIP*** **ENABLE MICROSOFT INTUNE CONNECTION**
>
> If you do not see the **Open A Ticket In Microsoft Endpoint Manager (For AAD Joined Devices) option**, you need to turn on the **Microsoft Intune Connection** in the **Endpoint Advanced Features** settings.

9. Select a **Remediation Due Date**.
10. Under **Priority**, select **High**.

11. Type some notes under **Add Notes** and click **Next** to open the **Review And Finish** screen shown in Figure 1-100.

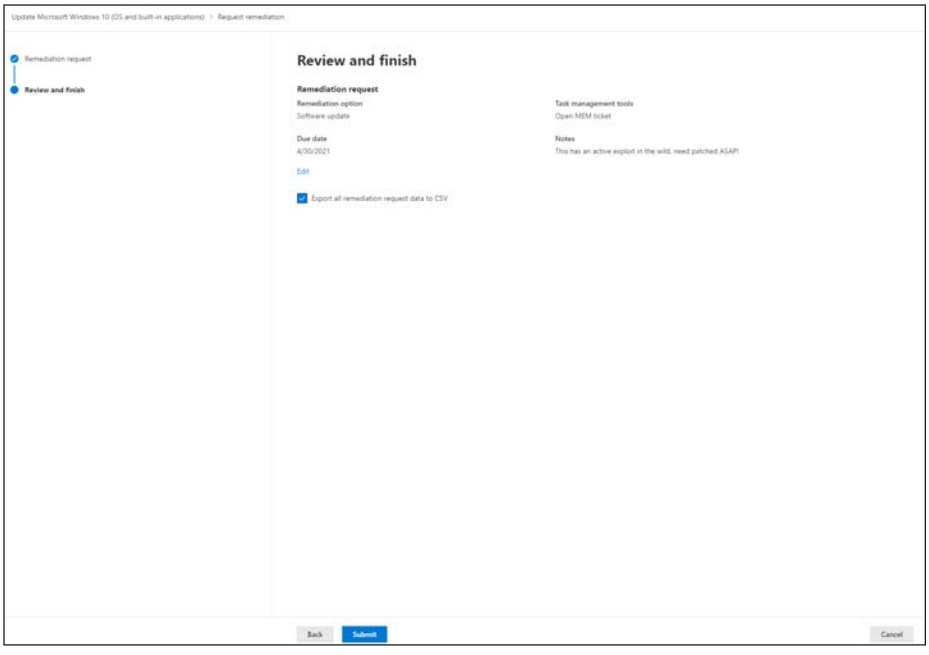

FIGURE 1-100 Review And Finish, Request remediation wizard

12. Select **Export All Remediation Request Data To CSV**. This creates a CSV file that you can provide with your change management request because it contains the remediation action and a list of the machines requiring the remediation.
13. Click **Submit**.
14. Once the remediation request is created, click **Done**.

Now that you have a remediation request created, you can track the request in the **Remediation** menu item under **Vulnerability Management**. Your patch management team should now see the remediation request in Microsoft Endpoint Manager under **Security Tasks**, as shown in Figure 1-101.

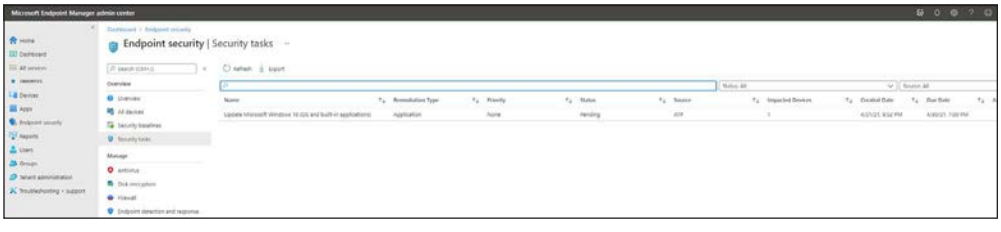

FIGURE 1-101 Security tasks in Microsoft Endpoint Manager

MORE INFO **REMEDIATE VULNERABILITIES WITH THREAT AND VULNERABILITY MANAGEMENT**

For more information about remediating vulnerabilities, see *https://aka.ms/sc200_tvmremedy*.

In some cases, you need to create an exception for security recommendations. For example, machines that do not support the hardware requirements for Credential Guard. Follow these steps to create an exception for these machines:

1. Log in to *https://security.microsoft.com* as a member of the **Global Administrator** or **Security Administrator** Azure Active Directory roles or as a member of an Endpoint role with the **Active Remediation Actions: Threat And Vulnerability Management—Exception Handling** And **Remediation Handling**.
2. In the menu on the left, under **Endpoints**, expand **Vulnerability Management** and click **Recommendations**.
3. In the **Search** option in the upper-right of the window, type **credential guard**. This should filter the security recommendation list as shown in Figure 1-102.

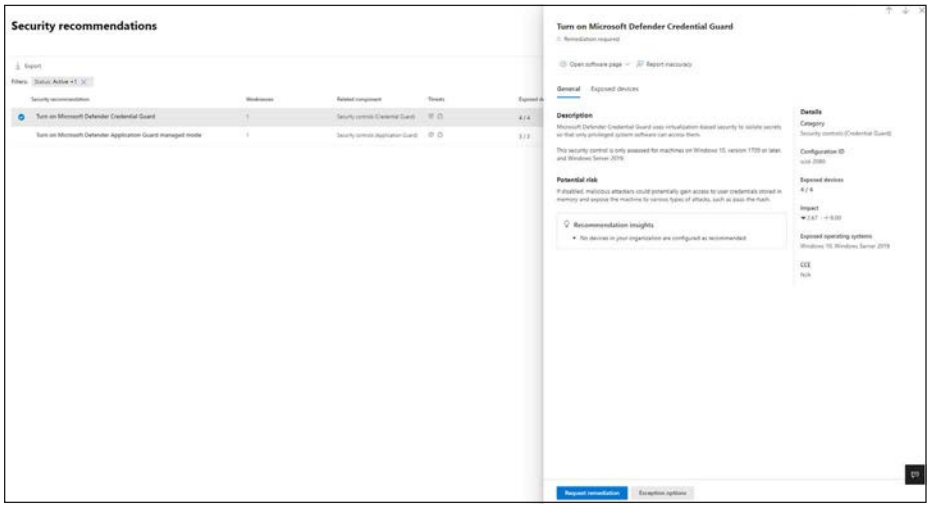

FIGURE 1-102 Turn on Microsoft Defender Credential Guard

4. Click the **Turn On Microsoft Defender Credential Guard** security recommendation. This will open a window with a description of the recommendation. Click the **Exception Options** button at the bottom of the window to open the **Create Exception** screen shown in Figure 1-103.