Microsoft

Microsoft Defender Advanced Threat Protection

Tutorial

Automated data classification

March 2019

Copyright

Introduction: AIP integration & data classification

Microsoft Defender ATP integrates with Azure Information Protection (AIP) enabling discovery, automated classification and protection of sensitive data stored on customers devices.

This scenario provides step-by-step instructions to run on your selected test machine to store, classify, and gain visibility on sensitive data stored on devices so you can explore and understand how Microsoft Defender ATP enables sensitive data classificiation.

The test machine required for this simulation must:

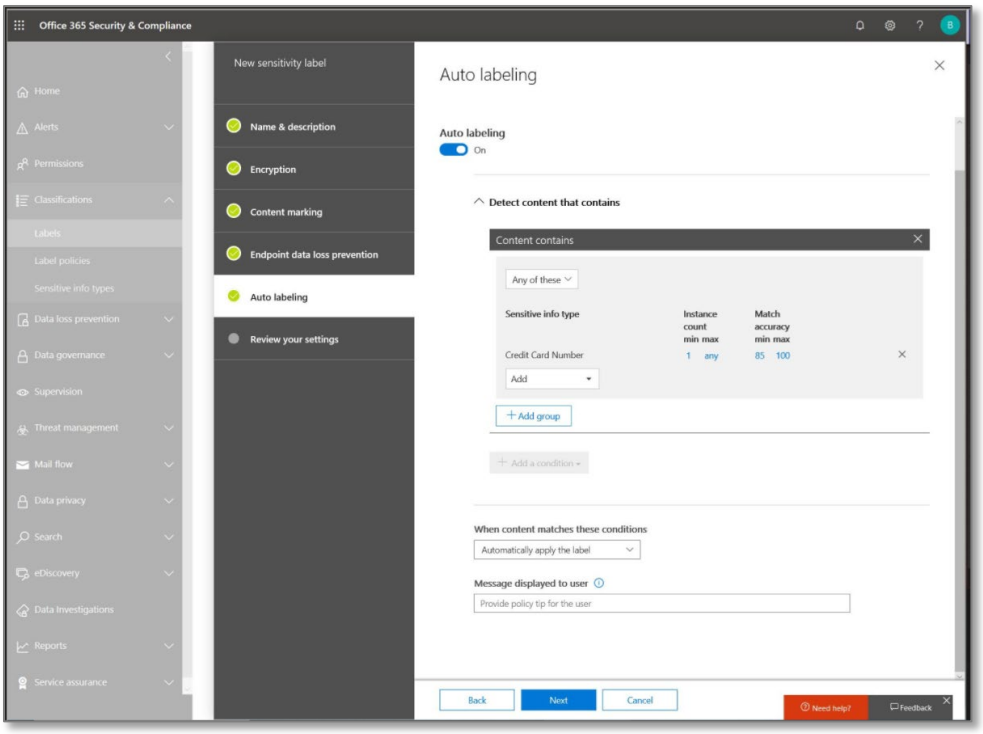
- Onboard to Microsoft Defender ATP
- Manage sensitrivity labels in Office 365 Security & Compliance Center (SCC)
  - Note: If you're using AIP to manage sensitivity labels please follow the label migration process
- Run the latest Windows Insider build
- Optional
  - Onboard to AIP analytics preview
  - Enable AIP integration in Microsoft Defender Security Center

For onboarding instructions, read to the product guide. We recommend running the local onboarding script to onboard the test machine.

Run the simulation

Configure classification and protection policy in Office 365 Security & Compliance Center

1. Create a new or select an existing sensitive info type label.
   NOTE: We recommend that you create a new label to avoid impacting existing labels or policies.
2. Click on **Edit label** to open the label settings.
3. Set a policy for Data classification.
   a. Go to *'Auto labeling'*
   b. Skip the Wizard steps until you reach the Auto labeling page.
   c. In the Auto labeling page, Switch *'Auto labeling'* on.
   d. Add a new auto-labeling rule that matches a '*Credit Card Number*' with a minimum instance count of **1**.
   e. Validate that *'When content matches these conditions'* setting is set to *'Automatically apply the label'*

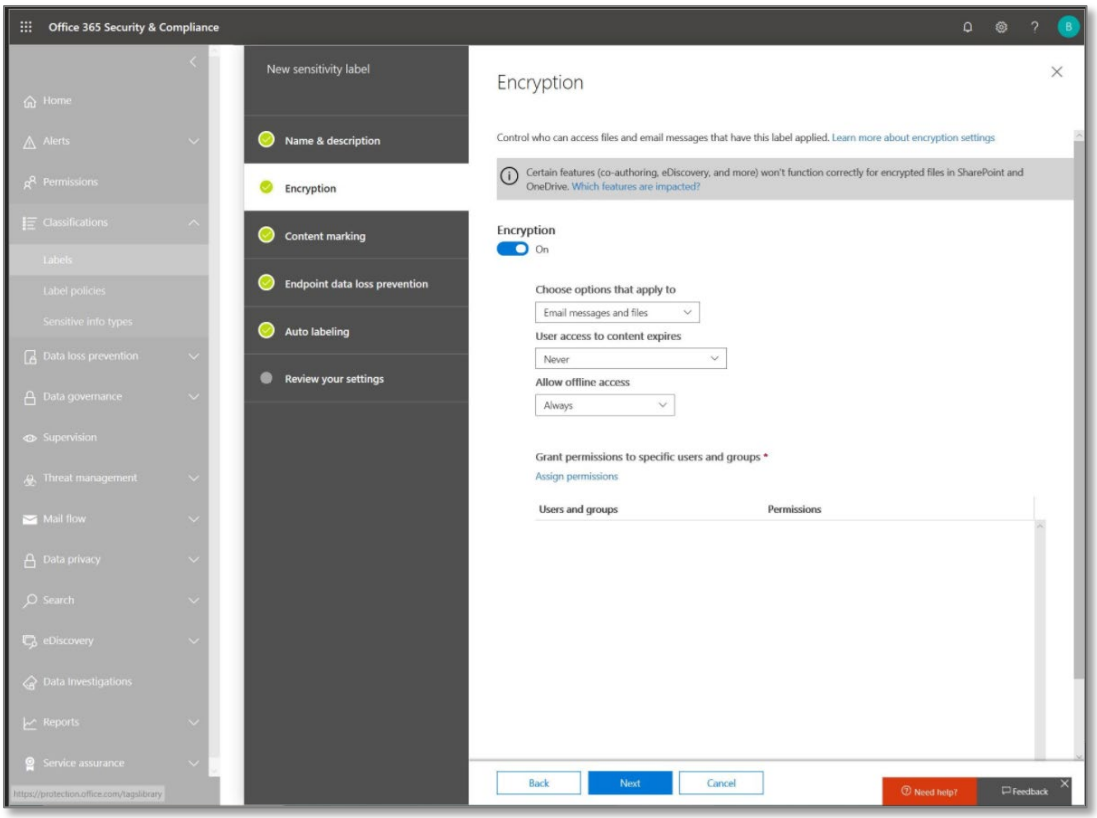


Auto labeling page in the security & compliance center

4. (Optional) Set an *'Endpoint Protection Policy'*.

    a. Microsoft Defender ATP integrates with WIP, using this integration customers can protect sensitive data based on lables.

    b. To enable protection, go to *'Endpoint data loss prevention'* and switch it **on**



Endpoint protection policy in the security & compliance center

Create simulation sensitive data on test devices

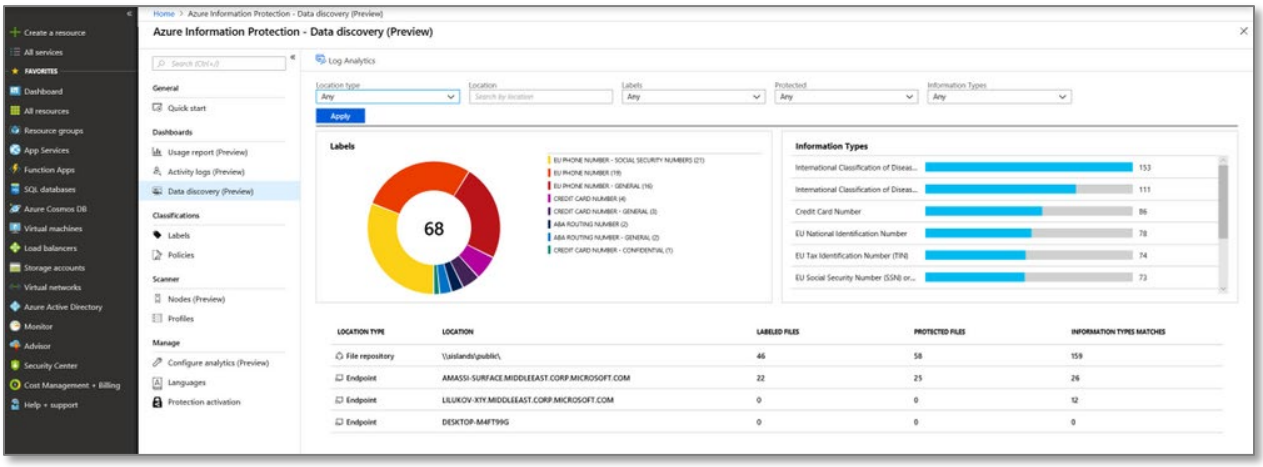
1. On the test device/s that's onboarded to Microsoft Defender ATP, copy the attached 'DLP_Test_Sensitive_File" test file.

   DLP_Test_SensitiveFile.csv

2. Microsoft Defender ATP will automatically detect the files containing sensitive data based on the classification policy created in the previous step.

Discover files automatically classified on devices

1. Open AIP Data Discovery dashboard.



2. See the discovery report.

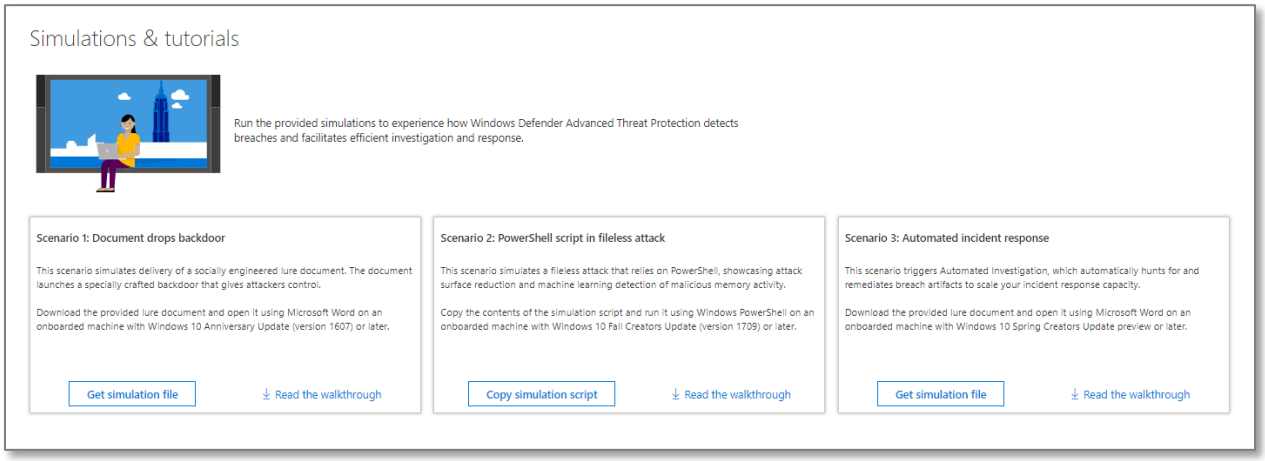
   a. On the data discovery tab , find the test device that was used in the previous scenario

   b. Click on the device , and view a list of files observed on this device, with their sensitivity labels and information types

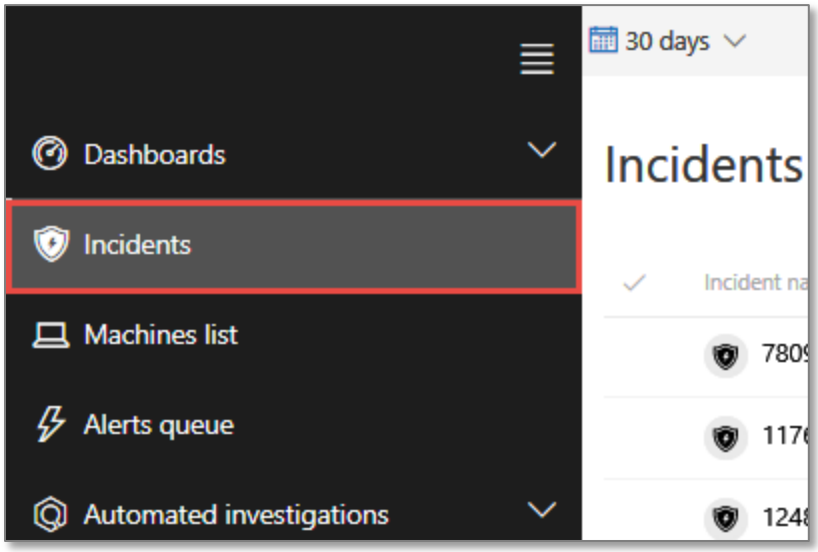
   Note: Please allow approximately 15-20 minutes for the AIP Dashboard Discovery to show the file you created.

Use sensitivity labeles to prioritize & investigate security incidents

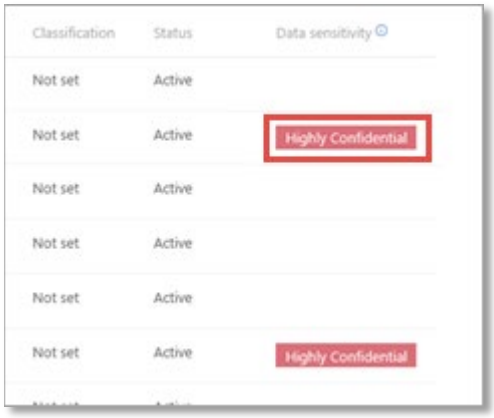
1. Log in to the Microsoft Defender ATP portal and go to **Help (?) > Simulations & tutorials**.



2. Run one of the attack simulation scenarios (Scenarios 1-3) on the test devices used for the automated classification simulation.
3. After 15-30 minutes of the simulated attack, you should find new incidents in the Microsoft Defender Security Center dashboard.
4. Open the the incidents queue.

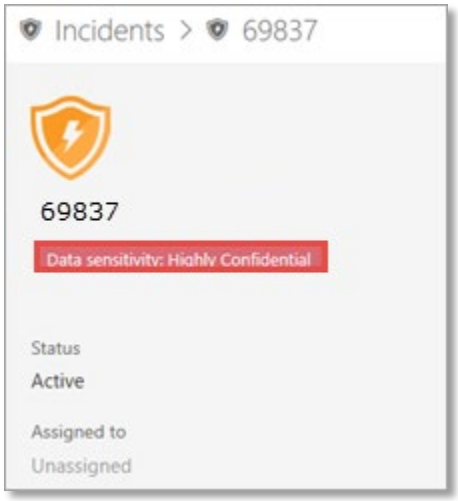


5. Scroll to the right and observe a new 'Data Sensitivity' culumn.

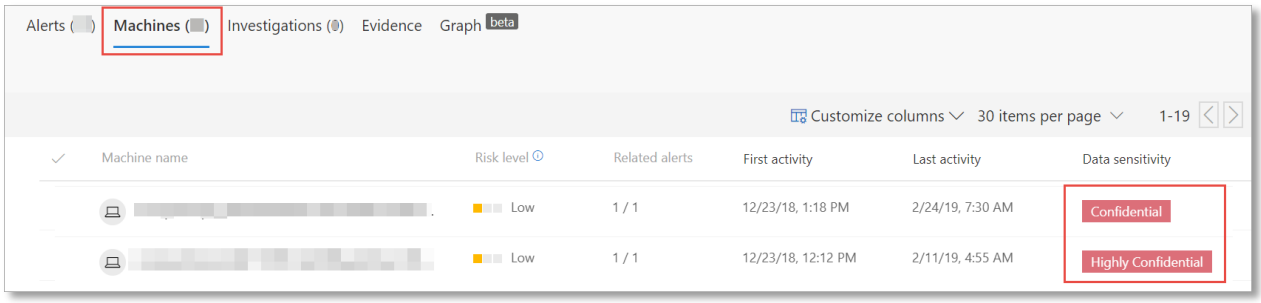


This column reflects sensitivity labels that have been observed on machines related to the incidents providing SecOps with an indication of whether sensitive files may be impacted by the incident as they prioritize incident investigation & response issues.

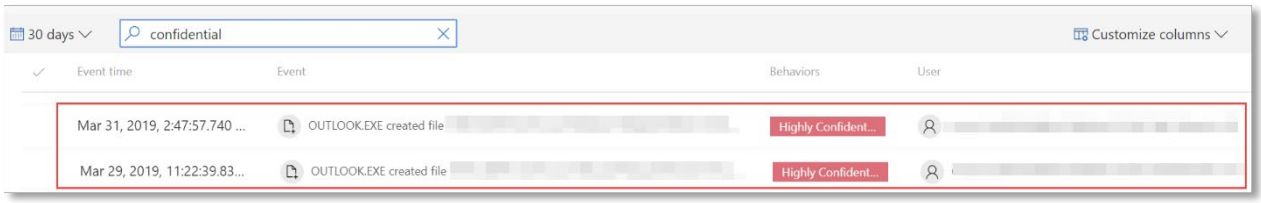
6. Open the incident page to further investigate. Note that the data sensitive attribution carries over into the incident page.



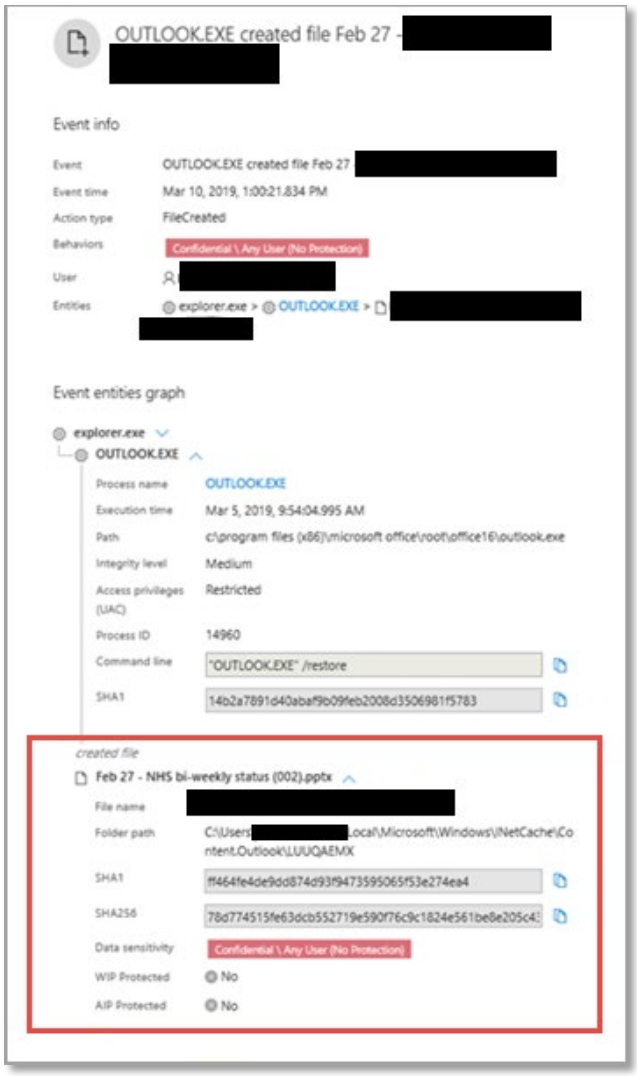
7. Click on the machines tab to identify machine storing files with sensitivity labels.



8. Click on the machines that store sensitive data an search through the timeline to identify which files may be impacted.



Note: The event side pane now provides additional insight to the WIP and AIP protection status.



9. These data points are also exposed through the 'FileCreationEvents' in advanced hunting, allowing advanced queries and schedule detection to take into account sensitivity labels and file protection status.

Conclusion

We've simulated how to use AIP labels and auto classification in order to automatically classifiy sensitive data stored on devices, and walked through how compliance officers can view the information via AIP discovery, and how security analysts can utilize this information to better prioritize and respond to security incidents.

We hope you enjoyed this simulation and are now encouraged to explore other features and capabilities. For more information, read the product guide at docs.microsoft.com.

Click the feedback icon on the Microsoft Defender ATP portal to let us know how you feel about this simulation or any other aspects of the product. We would love to hear your ideas about additional simulations and tutorials. Thank you!