|  |  |  |
| --- | --- | --- |
| Create an Activity Policy that will detect a suspicious activity such as mass downloading of files in a short timeframe. | | |
| Step 1 | Machine generated alternative text: MOD Administrator  Good afternoon  Search online documents  Install Office 2016  Other installs  Power 31  Mail  Delve  Calendar  People  Word  i;  Teams  Yammer  Dynamics 365  PowerPoint  Store  OneDrive  OneNote  MyAnaIytics  SharePoint  Admin  Planner  Security &  Compliance  Tasks  PowerApps | Log into you tenant  <https://login.microsoftonline.com/>    and the click on the Admin Center 'App' |
| Step 2 | Machine generated alternative text: Office 365  Billing  Support  Settings  Setup  Reports  Health  Admin centers  Exchange cf  Skype for Business cf  SharePoint cf  oneDrive cf  Yammer  PowerApps cf  Flow cf  Security & Compliance  Azure AD cf  Intune cf  Cloud App Security cf  Admin center  Home v'  Search users, groups, settings or tasks  Office 365 Enterprise E5 setup is incomplete. Get someone to help you.  Go to setup  ? MOD Administrator  Contoso EMS932138  Users >  Add a user  Delete a user  Edit a user  Reset a password  Videos  Admin center overview  What's new  > Admin mobile app  •oooo  Suggested features  Billing >  Total balance: None  In trial: Buy now  Message center >  Office software  Install my software  Share the download link  Software download settings  Troubleshoot installation  Domains >  Add a domain  Delete a domain  Edit a domain  Check health  Service health >  Some services have posted advisories  3 advisories  Active users  Q Support  —  'Planned Maintenance: SharePoint Online Read...  O Updated feature: Office 365 App launcher  New feature: Guest access in Microsoft Teams  sep 12  sep 12  sep 12  x  x  x  36 unread messages  Help users get started  Setup guides  New service request  View service requests  O Need help?  Feedback | In the left navigation, click on **Admin Centers** then click on **Cloud App Security** |
| Step 3 | Screen Clipping | From the Cloud App Security Home Page, From the **Control** menu, select **Policies** |
| Step 4 |  | **CLICK STEP(S)**  Click **Create policy**. |
| Step 5 |  | **CLICK STEP(S)**  Click **Activity policy**. |
| Step 6 |  | First, let’s select a policy template from the **Policy template** drop down menu.  **CLICK STEP(S)**  Click **Policy template** drop down menu. |
| Step 7 |  | As you can see there are a variety of templates to choose from.  For this demonstration, let’s use the **Mass download by a single user** template.  **CLICK STEP(S)**  Click **Mass download by a single user**. |
| Step 8 |  | **CLICK STEP(S)**  Click **Apply template**. |
| Step 9 | Screen Clipping | Now you can see that the template has been applied, filling out most of the essential fields.  Let’s continue reviewing the remaining policy settings.  **CLICK STEP(S)**  Click **scroll bar** to scroll down. |
| Step 10 | Screen Clipping | Since you are now developing a policy to monitor a specific type of activity “**Mass downloads by a single user”**, versus a more general anomaly/incident detection policy; the parameters which you monitor would naturally be more targeted.  This is where the **Create Filters for a Policy** section comes into play, allowing you to select the specific conditions that will trigger an alert.  In this case:   * The number of repeated activities is set to 50 * The timeframe which this occurs (measured in minutes) is currently 1 minute * Whether the activity comes from the same user or the same user/app.   Check out the different activities that are pre-selected and other options available under **Activities matching all of the following** |
| Step 11 |  | Moving on to **Alerts**.  **CLICK STEP(S)**  Click **scroll bar** to scroll down.  For this policy, let’s enable the **email alerts** and **Suspend user** options.  **CLICK STEP(S)**  Click **Email alert** checkbox. |
| Step 12 | Screen Clipping | **CLICK STEP(S)**  Click **To: field**. |
| Step 13 | Screen Clipping | Now that the Email alerts have been configured, let’s enable the **Suspend user** option by checking it’s checkbox.  **CLICK STEP(S)**  Under **Governance: Office 365**, click **Suspend user** checkbox. |
| Step 14 | Screen Clipping | Now the policy is ready for deployment. And we will have peace of mind that by the time we get this alert the user will have been automatically suspended.  **CLICK STEP(S)**  Click **Create**. |
| Step 15 | Screen Clipping | With the email alerts and the suspend user features enabled, you now have peace of mind; knowing whenever a user violates this policy he/she will automatically be suspended by the time you receive the email notification.  As you can see **Office 365 Advanced Security Management** provides you with enhanced visibility and control into your Office 365 environment though:   * The ability to detect threats by helping you identify high-risk and abnormal usage, security incidents, and threats. * Providing you with enhanced control by leveraging granular controls and security policies that can help you shape your Office 365 environment. * Giving you enhanced visibility and context into your Office 365 usage and shadow IT though the discovery and insights that the solution provides, all without installing an end point agent. |