|  |  |  |
| --- | --- | --- |
| Create and Anomaly Detection Policy that will monitor and detect admin activity anomalies and send an alert / text message when a specified threshold is reached. | | |
| 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 **Anomaly detection policy**. |
| Step 6 |  | For this policy creation, let’s use the following values:   * **Policy template**: Let’s leave it as **No Template** * **Policy Name** will be **Admin Activity** * Description: **Will be Monitoring Admin Activity for Anomalies** * Category: Will be left as **Threat Detection**. |
| Step 7 |  | * Activity filters: Will be changed from **All monitored activity** to **Selected Activity**   **CLICK STEP(S)**  Under Activity filters, click **All monitored activity** drop down menu. |
| Step 8 |  | **CLICK STEP(S)**  Click **Selected activity**. |
| Step 9 |  | **CLICK STEP(S)**  Click **Select a filter…** drop down menu. |
| Step 10 |  | **CLICK STEP(S)**  Click **Administrative activity**. |
| Step 11 |  | Now that the Activity filter has been set, let’s move on to the **Risk Factor** section.  This section contains a total of 8 subcategories:   * Logon Failures * Admin Activity * Inactive Accounts * Location   **CLICK STEP(S)**  Click **scroll bar** to scroll down. |
| Step 12 |  | * Impossible Travel * Device and User Agent * Activity Rate * Risky IP Address   All of the subcategories within the Risk factor section can be left to their **default setting of on,** as you see them now, turned off or applied to specific activities.  Now let’s move on to the **Alerts** section.  **CLICK STEP(S)**  Click **scroll bar** to scroll down. |
| Step 13 |  | Within the Alerts section, you have the ability to set the Alerting threshold and enable email/text alerting.  To get a better understanding of Alerting threshold, let’s uncheck the Alerting threshold checkbox to expand this section.  **CLICK STEP(S)**  Under **Alerting threshold**, uncheck the **checkbox** “Use default severity threshold settings (recommended)”. |
| Step 14 |  | **Alerting threshold** is a numeric value that will determine when alerts are generated.  The generation of alerts depends on what the Risk score bar below is set to.  The default score is 65, which means that any incidents with a Risk score of 65 or higher will generate an alert.  For this HOL, let’s set the Risk score to 85.  **CLICK STEP(S)**  Slide the **Risk score bar to 85**. |
| Step 15 |  | Now let’s move on to the **Alerts** configuration section.  Here, you have the ability to alter how many alerts you receive daily, enable email alerts and/or sending alerts via text message.  If you click on the Daily alert limit drop down menu, you can set your daily alert limit to any of the following values.  **CLICK STEP(S)**  Under **Alerts configuration**, click **Daily alert limit** drop down menu. |
| Step 16 |  | For today, let’s leave the daily alert limit as it’s default value of 5.  **CLICK STEP(S)**  Observe the options in the dropdown and select 5. |
| Step 17 |  | Now let’s configure the email and text alerts.  To enable email alerts, first check the checkbox.  **CLICK STEP(S)**  Click **Email alert** checkbox. |
| Step 18 |  | Then enter a valid corporate email address and hit Tab.  And yes, you are also able to enter multiple email addresses as well.  **CLICK STEP(S)**  Click **To: field** and enter a valid corporate email address. |
| Step 19 |  | Email alerts have been configured, let’s move on to configure the text message alerts  **CLICK STEP(S)**  Click **Send alert as text message** checkbox. |
| Step 20 |  | As you can see, the phone number field provides you a template to follow.  If you do not use the correct phone number format, you may receive an error message when you attempt to create the policy.  **CLICK STEP(S)**  Click the **phone number field** and enter a phone number in the specified format. |
| Step 21 |  | Now that the policy configuration is complete, it’s time to deploy it.  **CLICK STEP(S)**  Click **Create**. |