The Risk demonstration

Introduction

This demonstration is pre-configured on the IdentityIQ 6.1 Partner VM.

Demo startup

1. Open up different Firefox browser sessions and log in as the following players:
   1. Amanda Ross (leave at Dashboard).
   2. Jerry Bennett (navigate to Manage / Identity Risk Scores / High Risk).
2. Open up “Active Directory Users and Computers” and select the “TreasuryMgmt” group.

**Tip:** Open up a DOS box. This way, the new DOS window will appear largely behind the existing one and your task is completely hidden. You will be able to tell the task has finished by the small change in the icon.

 versus 

The Risk Demo Scenarios

1. Go to the Browser session for Jerry Bennett and show the current high-risk users. Note that Henry Butler is not amongst them.
2. Add Henry Butler to the “TreasuryMgmt” group in AD using “Active Directory Users and Computers”.
3. Save the change in AD and then hit the key combination “Ctrl-Alt-1” to start the aggregation and cube refresh.

**Note:** The minimized “DOS Box” in the task bar will open while running, and disappear when the task is finished. You will need to discuss the following while the task is executing.

**Talking Points During Task Execution:**

* Talk about why static risk tagging does not work. For example: Person 1 has 10 entitlements with risk 100 each and becomes a risky person with a risk score of 1000 in total. But Person 1 needs this access to perform his/her job and all access is approved through a certification or approval process.  
    
  Person 2 has only two entitlements, and as a result person 2 has a risk score of 200. But because entitlement 2 is not required and has not been approved, this person actually is the more risky of the two users.  
    
  That entitlement in itself only has a risk score of 100. But thanks to the model, it grows out into high risk, as access has not yet been approved.
* Talk about the risk model and how it will now detect a change and because access has not yet been approved, this risk level of the entitlement we just added to the user is actually multiplied, resulting in a high risk.

1. Refresh the High Risk window using the refresh button and show how Henry has now become a high-risk user.  
     
   **Note:** It is good to highlight that the Risk model can be tuned to your liking without any impact. Out of the box, you have to take manual action.   
   For this demo, we tied Risk into the Policy Model, using a Risk Policy to trigger a newly created workflow. The workflow is simple. It merely asks the manager to perform an access certification for the user.
2. Go to the Amanda Ross browser session and refresh her inbox (Click on the Dashboard link).
3. Go into the Risk Review for Henry Butler and certify his access.
   1. Approve the two roles, but revoke the TreasusryMgmt entitlement, as this is not appropriate.
   2. After approval / revocation go back to the identity view and click the sign-off button.
   3. Hit the key combination “Ctrl-Alt-2“ to start the maintenance task (to close off the certification after sign-off) and refresh the cubes.
4. Show in AD how Henry’s access has now been revoked (no longer a member of the group)
5. After the task has finished, as Jerry, show how Henry is no longer a risky user by refreshing the High-risk view.

Other Options for the Risk Demo

* + - 1. Run the Policy Violation report immediately after the Ctrl-Alt-1 task has completed, to show the outstanding violation as a result of the demo rule.
      2. Create a “Identity Risk Live report” to show High Risk users before and after the remediation.
      3. After the demo, show the snapshots on the Identity Cube for Henry.Butler. The latest snapshot should indicate he was previously a member of the PayrollManagerAccess group.

History

|  |  |  |
| --- | --- | --- |
| Date | Changes | Comments |
| June 23rd 2012 | Initial version |  |
| August 12th 2012 | Aligned to naming convention |  |
| December 4th 2012 | Updated for IIQ 6.0p1 and latest demo environment |  |
| October 30, 2013 | Updated for 6.1 Demo scenario | Removed set-up instructions as this is part of the shipping image |