Vasco, Pietto (NE)

From: Ellsworth, Jarrod T
Sent: Monday, October 31, 2022 1:25 PM
To: Vasco, Pietto (NE)
Subject: Test - Enable File Auditing On Single Windows Server

Pietto,

I took some time to look into https://jira.ccwdata.org/jira/browse/INF-11293 and have some follow up.

The Tech Spec needs to be filled out. What did you do to satisfy the Acceptance Criteria. For this card you created a script that set a group policy item or you launched gpedit.msc and made that change. That's what needs to be in the Tech Spec. In addition to setting that group policy setting you also had to either script or manually change the permissions on the system32 folder to enable auditing of that folder once the policy setting was configured. This should all be a part of the Tech Spec.

As for the auditing of the folder there are some issues.
I see the principal is TEST\authenticateduser. Is manually typed or did you use the GUI where you click the Check Name button that fills that in? I'm asking because it doesn't look right on the folder properties.
Also, I think we want to audit for everyone not just authenticated users.
If you are setting these permissions programmatically there are well-known SIDS for Authenticated Users and for Everyone

We are trying to monitor for changes to this folder. In the Advanced Permissions for auditing I see that Read attributes and Read extended attributes are checked but Delete, Delete subfolders and files, Change permissions, and Take Ownership are all unchecked. That should be just the opposite.

Once that auditing is configured correctly there should be a list of Event IDs that we can look at to see how often files are being modified.
This page lists the event IDs: https://www.lepide.com/how-to/track-changes-made-to-your-files-and-folders.html

I searched for the following Event IDs in the Security log on tscw10ap24 and there 0 results so I'm not sure if that auditing is working correctly.

4658,4660,4663,4685,4985,5140,4656,4658,4659,4660,4663,4664,4691

I know you compared the number of events over a few days from before you made the change that may have just been an anomaly or normal fluctuation.

Thanks,

Jarrod Ellsworth

Systems Engineer Advisor
General Dynamics Information Technology, Inc.
1401 50th St. Suite 200
West Des Moines, IA 50266
(515) 226-1841 Office
(515) 440-3159 Fax
jarrod.ellsworth@gdit.com
www.gdit.com