

RE: When IT Manager breaks rules

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-05/msg00408.html>

- *From:* "Robinson, Sonja" <Sonja.Robinson@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 18 May 2007 15:38:56 -0400
-

You can dump your domain controller event logs using something like dumpiest (you should probably be saving these anyway for SOX/HIPAA/GLBA compliance). Then search for the appropriate security event code on a weekly basis. Anyone who entered the items that were unauthorized get investigated. This should be a routine process. Search for members added, deleted, changed. Search for group memberships added to see whose rights were added and deleted and if appropriate (eg. who was given rights they should not have been). Search for audit policy changes, domain policy changes, etc. If you review these items on a routine basis it is an objective way to "catch" policy violations and prove you are auditing and monitoring your systems.

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]
On Behalf Of Shawn
Sent: Friday, May 18, 2007 10:29 AM
To: WALI
Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx;
security-basics-return-44419@xxxxxxxxxxxxxxxxxxxxx;
security-basics-return-44427@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: When IT Manager breaks rules

Thinking on this further, you may even be able to skip the VBScript/scheduled task thing...you **may** be able to do this with built in M\$ stuff.

I **think** you can set up an alert in Performance Logs and Alerts to fire whenever an account is created. You'd want to monitor the "NTDS" object for account creations.

The advantage to this would be less system resource use, as you wouldn't have to periodically run a VBScript.

-Shawn

On Thu, 17 May 2007, Shawn wrote:

This should be very easy to implement. Perhaps the easiest solution:

RE: When IT Manager breaks rules

1. Configure auditing via group policy to log an event each time a new

account is created.

2. Drop a VBScript in your domain controllers scheduled tasks that reads the security log and sends you an email each time an event is recorded for a new account creation.

We have a much more complex solution for the same issue here, using HP

OpenView...basically part of our enterprise wide centralized alert system.

But you don't need a \$60,000 piece of software to make this happen.

-Shawn

On Thu, 17 May 2007, WALI wrote:

Hi guys...an odd question here!! I am mad at my IT Manager, he is such a sissy!!

Being a internal security analyst in-charge, I want to enforce a few policies at help desk. One of them is, not to create any user account

unless an email arrives from HR to HelpDesk, informing of the user's badge ID, the department he/she belongs to. The status of employment and all those things. The procedures are in place but sometimes it so

happens that some Head of the Dept. or executive management calls up our IT Manager over the phone, or send him an email directly which is

then forwarded to our Help Desk incharge who is then left with little

RE: When IT Manager breaks rules

options but to create the account without due processes. All policy compliance guidelines get thrown up in the air.

HelpDesk incharge is bound by his position to, not to defy IT manager

and he is scared to tell me (sometimes he does) that IT manager is forcing him to dilute the AD account creation policy.

I don't want to confront IT manager based upon inputs by Helpdesk guys but would rather put a mechanism in place, where I would automatically come to know, that an account has been created and I can ask helpdesk to provide proof of the email from HR arbitrarily

and then confront the manager.

I know some Audit trails can be put and they would appear under Security tab of Event manager (or so I guess) but I need something more automated that would land in my mailbox.

Is this possible through any automated solution in AD of Windows

2003?

Probably MOM 2005 or the types?

In case I chose to confront HR Admin/ managers with a plea to stop sending such requests to our IT Manager and put their house in order,

what all genuine risks of 'not doing so' can I highlight? Ours is fairly large corporation employing about a 1000 people.