AD Administrative Practices Walkthrough

Monday, December 6, 2021

1:02 PM

Attendees:

Machine generated alternative text:
Oluwaseyi Mafi 
Ann Marie French 
Bianca Moon 
David Kaemmerer 
James Rose 
C) Joseph Rocha 
Mark Ostrowski 
O Michael Shanahan 
Sarah Kubiak 
Saurabh Dilip Saxena 
c) Terri Ann Quiambao 
Tyrell Jarrett 

Location: Webex

Date: 12/6/2021

AGENDA

**Understanding how the admin account password vault process operates.**

Jim: Broken up by Job role.

Mark: When an individual account is to be granted access. Goes through the same process, by MyIT, from manager and owner of such group. Domain access, IT request processed then goes to Mark as owner of the group. We follow the standard process for provisioning account. There is traceability. We go beyond that. The implementation process is getting stricter. Has to get approved through several approvals. Sometimes it is temporary or permanent. We have an annual PAR process. Mark owns Domain access group. Manager approval, then goes through Mark, or additional approval (determined by MyIT, IAM). Final approval comes from the group owner.

Active directory access, privileged access - owned by Mark. No approval is granted to a user account. It has to be privilege account.

**What is the process for user to get admin access?**

Mark: Same provisioning process by IAM.

Jim: It is different form PSS and HCB. There are default group we all utilize. The approval process for Admin account. We currently don't have an enterprise workflow. Everything must be approved. HCB, PSS etc have a different process. HCB has an approved process come in, more of a two-layer tier. We have segregated system we are getting better at.

Jim: It will get integrated into SNOW. Very restricted, and owner will sign off on it.

There is segregation of admin and user accounts. MA account and ZZ account. ADM account on the PSS side. We have password vaulting for admin account. These accounts require multifactor authentication. Account are restricted. Far more stringent.

There are different admin accounts, hence access is not shared. There are default IDs for everyone who takes ownership and is responsible for gaining access, termed Break fix account. This is a global initiative.

Mark: Because of PCI, everything is logged.

**What is being logged?**

Mark: When individuals log in, and check out, it is logged. We do not review the logs. Falls under the security operations centers for review.

A privilege user cannot look up emails using an admin account, but rather these are blocked.

Mark: Just because I have domain right, doesn't grant access to other rights.

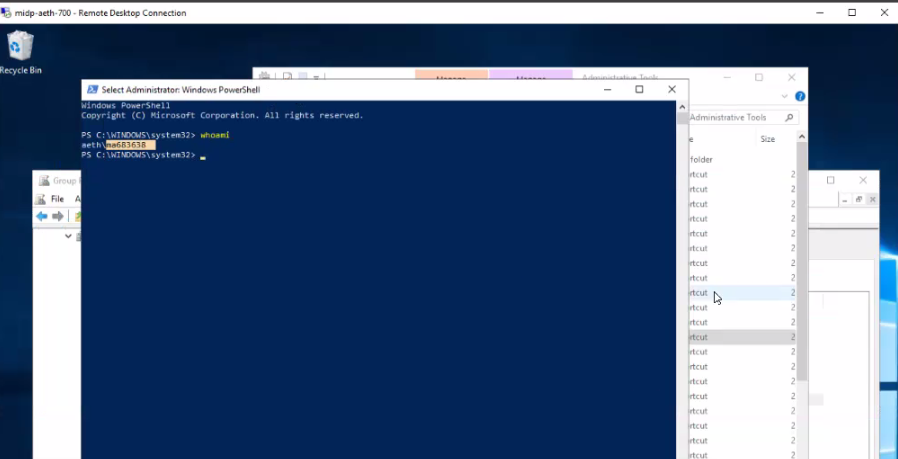
**How do you segregate certain users from having access?**

Domain admin only have read, right functions.

Jim: Directory info are specific. Access is generally through a group.

Machine generated alternative text:
9Wp 
2-2 
"TOS 
OSX 
mput 
c o 'Vine to r 
Odwtt SIDS 

Machine generated alternative text:
o 
C•my policy 
P.bcy 
D Pdicy 
tuning 
Policy 
Adm. n & I icy 
AWNPTOC 
Advanced Audit Configuration policy 
CON rRCLLER_S 
* SYSTEM 
GPO 



Domain account.

All privilege admin accounts should be password vaulted.

**LOGGING AND MONITORING WALKTHROUGH PREP**

IAM team would be responsible for the password vaulting. Michael Shanahan will step in to provide details on the SME for this aspect.

We do not own the monitoring aspect; it is part of the EIS team. These individuals should be brought into the call. Contact Michael Shanahan.