Team: Team 8

Inject Number: 23

Inject Duration: 30 Minutes

Inject Start Date/Time: Sat, 13 Feb 2021 17:31:46 +0000

From: IT Director

To: SOC Staff

Subject: IMAC - Windows Admin Accounts Report

The Security Director raised a concern about enabled Active Directory administrator accounts. The concern is that there are administrator accounts that are potentially active and should have been disabled. Please run a PowerShell command to generate a list of domain admins and annotate if they are enabled accounts. In a business memo, provide screenshots of the powershell output showing the enabled/disabled administrator accounts. Be sure to show the powershell commands used.

Thank you.

IT Director