Policy 5.10 Progress Overview

Task	Tools to Identify and Classify Systems	Potentially Useful Classifications	Remediation Strategies

Patching	• FileMaker Pro (find functionality)
	• Active Directory CM
		• In AD (thus, have CM) and networked
		  ◦ Patched automatically and fully
		  ◦ Not automatic - provide reason
		• Not in AD and networked
		• Airgapped (no recent, live data)
			If not automatic, make automatic. Else:
			• Document as justifiably non-compliant.

Encryption	• FileMaker Pro (find functionality) • Active Directory CM • LastPass keys	• Encrypted & required • Encrypted & not required • Not encrypted, but required • Not encrypted & not required	Primary concern: "not encrypted, but required" systems. Must make compliant. Any way to automate such systems' encryption?

Screen Lock	• FileMaker Pro (find functionality)
	• Active Directory CM
		• Networked
		  ◦ 10-space
		  ◦ Full IP Address
		• Not networked
			Current solution: manually verify non-networked systems for screen lock compliance.

Understanding Main Considerations

To understand the most important aspects of the policy, it is necessary to first understand the status of devices most likely affected by the policy before proceeding with more complicated scenarios that require more considerations. Thus, this section will deal primarily with Windows desktops and Windows laptops. Furthermore, this section will focus on the policies that are most likely to affect the Chemistry IT department: Patching, Encryption, and Screen Lock.

Critical Computers

Windows laptops and desktops are the primary concern. However, not all windows laptops and desktops in the inventory are useful, for many inventoried laptops and desktops are missing, scrapped, or in the stock room. Therefore, when talking about windows laptops and desktops that likely have some relevance (by not being stock, missing, or scrapped), this page will refer to them as "critical computers."

Patching

According to the policy, patches must be applied within 14 days of release. It is possible to use Active Directory's CM Client to verify which systems undergo a "Managed Update." Thus, the primary concerns are:

1. To identify which critical computers are in Active Directory without "Managed Update"; and
2. To identify which critical computers are not in Active Directory, for those are the systems whose patching status cannot be automatically verified.

Current Solution to Patching Concern #1

As of early October, 2017, there were 111 critical computers with Managed Update. Therefore, to answer how many critical computers are in AD, but not undergoing Managed Update, all that is needed is to subtract 111 from the number of critical computers in AD. This can be done by searching the inventory for critical computers that follow the "AS-" naming convention (which means it is in Active Directory) and subtracting 111 from the number yielded from the search. The resulting number would be the answer to how many systems are in concern #1.

To generate the list, assuming the inventory search is dependable, perform the above search and generate an excel file. Then bring to that file the list of systems undergoing Managed Update and compare. The list of systems in the search that are not in Managed Update should be as large as the number of systems in the search subtracted by the number of systems in Managed Update (111 as of early October, 2017).

Current Solution to Patching Concern #2

To identify which critical computers are not in AD, simply perform an inventory search for critical computers that don't follow the naming convention (resulting number as of October 20, 2017: 313). The resulting number of systems should be the same as the number of critical computers (596) minus the number of critical computers in AD (283) ==> 313.

Encryption

The policy states that laptops and desktops must have whole-disk encryption, except for those that are Virtual Machines, Instrumentation Machines, systems that are automatically reconfigured, and data-less workstations. However, despite these official exceptions, the policy requires that all exceptions be documented. Therefore, it is important to somehow keep track of these machines and systems that likely will never get encrypted. Another use for keeping track of this information is that it will allow us to know which excepted laptops and desktops are encrypted nonetheless.

Thus, the encryption concerns are like that of Patching, but with the twist that we don't concern ourselves with excepted machines in remediating policy violations but are still expected to track which systems we don't concern ourselves with for remediation strictly for documentation purposes. Thus, the primary concerns are the following:

1. Finding out which non-excepted critical computers are not in AD
2. Finding out which excepted critical computers are in AD and are encrypted.

Current Solution to Encryption Concern #1

Simply perform a search of critical computers whose function is not instrumentation or virtual machines and whose machine name is not the naming convention (starting with "AS-") to arrive at a tentative list of computers we might be concerned about since we can't verify encryption status if not in AD and since it is not excepted (and therefore must be remediated if not compliant).

Current Solution to Encryption Concern #2

This will require getting a list from AD of all critical computers that are encrypted and generating an excel file from inventory of all critical computers whose function is not instrumentation or virtual machines and whose machine name follows the naming convention. Then, match up the two lists and find out which ones are in common to solve concern #2.

Screen Lock

5.10 mandates that all computer systems not in a secure, private space run a password-protected screen saver that is automatically triggered after 15 minutes of inactivity.

Our main efforts, then, will be to eliminate systems that are typically in secured locations (such as instrumentation machines) from our search to refine which systems are at most risk, and therefore need more immediate attention for remediation. Thus, our primary concern is the following:

1. Find out which non-secured critical computers are not in AD.

Current Solution to Screen Lock Conern #1

So far, we know to conduct a standard search of critical computers not in AD, but with the caveat that they also not be instrumentation machines (as these are tyically secured).

Remediation

Edge Cases

After we have gathered enough information and have started/almost finished remediation on critical computers of primary concern, then we can deal with edge cases, including: other operating systems, exceptions, etc. We simply need to focus our efforts on more important considerations before having a complete implementation of the policies.