# CSIS 230- Active directory Security Case study

In your role as a systems engineer or security professional, you will undoubtedly be tasked with building, monitoring, and maintaining the security of the Active Directory infrastructure. Active Directory provides a long list of critical functions and services throughout the network. However, given its role in sensitive functions such as managing users, devices, critical services, etc., it is essential to be actively engaged in following security best practices, and to be aware of unique circumstances that may exist for your organization.

### You can reference the “Top 25 Active Directory Security Best Practices” document provided in Canvas, and you will also have to conduct research to find additional sources. **Be sure to cite all sources in your writing, and use APA reference style for your references in the last section.**

### Type directly into the gray boxes only. The boxes will expand as the paragraph grows. **Keep this document saved in a safe and accessible location as you will be completing one section per week, on average, as you go through the course.**

### Each content Section is worth 15 points total. Your reference list and proper citations are worth 10 points. This assignment is worth 100 points total.

### For each of the following areas of Active Directory Security, please provide the following:

### An overview of the concept, including why it is important to the organization (5pts)

### Best practices for addressing the issue (5pts)

### Potential harm to the organization if left vulnerable (5pts)

### **Domain admin Group**

**Your Response:**

|  |
| --- |
| The Domain Admin group are security group that is created automatically when create an Active Directory domain. The predefined groups can be used to help control access to shard resources and to delegate specific domain-wide administrative roles. So having another individual who is also apart of the Domain Admin Group allows, if person out that any changes need be made there’s always a back up person. By only having one induvial over the Domain Admin Group, they can make any changes that they want not be held responsible. |

### **Use of standard and Administrator Accounts**

**Your Response:**

|  |
| --- |
| When it comes standard account is your everyday employees that need to run multiple programs on the computer, but they have limited or restricted access to administrative access to computer. With Administrator accounts is for the user who to have full control over the computer and attain complete access, this should set creatin group individual’s having access. If the standard users dose not restricted access it can lead major issue down road if some reason that user was be hacked could create a lot damage on the network.  That being said there a lot issue that came about with a Administrator account as well if wrong individual in role can cause major of damage as well, that need trusted individual be admin should not allow everyone to be a admin with the company. |

### **Securing the domain administrator account**

**Your Response:**

|  |
| --- |
| With every domain they always include an Administrator account, which by default is a apart of the of Domain Admins group. The Admin account should only be used for domain setup and disaster recovery (restoring Active Directory). It is vital that no one know the Domain Administrator account password. There are some practices that can be done protect it, one is enable the account as sensitive and cannot be delegated, another practice is to require smart card so that login is interactive and make brute force attack hard to comment. You can also deny logon as batch job, also logons through RDP. If you leave this account open and the wrong person where to access it could corrupt the disaster recovery that was stored, and cost company ton of money. |

### **Securing the local administrator account (Include LaPS)**

**Your Response:**

|  |
| --- |
| Local Administrator accounts automatically installed within a windows computer, they are considered necessary to be able run system updates, software upgrades, and hardware usage and helpful to gain local access to machines if the network goes down. Having the LAPS open allow chance for the hacker to be able to gain access it preform a massive attack on the network form gaining access to the LAPS. To solve issue with LAPS that can occur you can go and eliminate the local admin accounts altogether making everyone a standard user. By doing this employees will have to wait for permission causing delays and productivity loss. Other option is retaining the accounts and manage them properly, which would require a lot of careful planning and management and maintenance to mitigate the risks. If you go with the last option then the passwords should be strong, unique, and periodically changed. |

### **Audit policy settings for Group Policy**

**Your Response:**

|  |
| --- |
| The audit policy setting for group policy can affect all computers and servers. It is important to have audit because it will allow you know if their issue with network and makes pin pointing it down easier where the issue is coming from. Some of the audit practice that can be done one is for account logon, ensure ‘audit credential validation’ is set to ‘success and failure’, another important is privilege use audit ‘sensitive privilege use’ is set to ‘success and failure’. By not having audit policy’s set it makes easier for bad actor to slip underwire before harmful actives to your companies’ network. |

### ***Select one additional best practice of your choice:***

**Your Response:**

|  |
| --- |
| Use two factor authentication for office 365 and remote access, this using either using physical item that constantly is changing number attached to it that must be entered before user can fully login or code is sent to there phone. By doing this it helps prevent account being compromised by bad actor and help create better security for your company. If that did not implement it does make it easier for bad actor to infiltrate due factor you are not getting dinged stating that user is trying access this login if they correct info they are going get in right away without issue. Example I’m able to provide is that with battle net account with blizzard I have authenticator attached to it which on my phone has app that dings if anyone is trying login into my account I can deny access for it form my phone also when I’m logging in it dinging my letting me know asking I’m aware allowing access to it. |

### **References** *Please provide a bibliography of the sources cited throughout your project.*

**Your Response:**

|  |
| --- |
| Dansimp. (2022, October 5). *Active Directory Security Groups*. Microsoft Learn. Retrieved February 19, 2023, from <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>  Ballmer, S. (2023, February 5). *Standard user account vs administrator account what's the difference*. Standard user Account vs Administrator Account what's the difference. Retrieved February 20, 2023, from <https://windows101tricks.com/standard-user-vs-administrator-accounts/>  Allen, R., Leandro, Hina, D., Ale, Kuskowski, E., ce1, Rick, Edward, Minh, Ivanoff, M., David, Inky, William, Fenrizx, Kelly, B., Lilov, V., Geekgal, Ren, Byron, … Samir. (2022, December 21). *Top 25 active directory security best practices*. Active Directory Pro. Retrieved February 27, 2023, from https://activedirectorypro.com/active-directory-security-best-practices/#secure-domain-admins  Viswanathan, Raja. “Best Practices for Managing Local Admin Accounts to Minimize Security Risks.” *Local Admin Accounts - Security Risks and Best Practices (Part 1)*, https://www.securden.com/blog/local-admin-accounts-management.html. |