Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *From the event log, it's evident that the incident occurred on 10/03/2023 at 8:29:57 AM,* ● *The event was initiated by the user "Legal\Administrator" from the computer "Up2-NoGud" with the IP address 152.207.255.255.* ● *These details will help in identifying the threat actor.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *Overly Privileged User: The incident points to a user with the role of "Administrator" having access to payroll-related functions. Administrators typically have extensive privileges, and in this case, they may have had more access than necessary for their role.* ● *Inactive User Accounts: There is a possibility that the account associated with "Legal\Administrator" should have been inactive or closely monitored, especially for payroll functions, to prevent unauthorized access.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Role-Based Access Control (RBAC): Implement Role-Based Access Control to ensure that users have the minimum necessary permissions for their job roles. Restrict access to sensitive functions like payroll to a specific group of employees, reducing the likelihood of incidents like this.* ● *User Account Review: Establish a regular review process to assess the necessity of user accounts, particularly those with elevated privileges. Ensure that accounts are deactivated when they are no longer required, reducing the risk of unauthorized access by inactive accounts.*