Access Control

	Note(s)	Issue(s)	Recommendation(s)
Authorization /Authentication /Accounting	***Event logs can often help you identify the who, what, and why of a security incident. My notes in short bleow***: ● *The event took place on 10/03/23.* ● *The user is Legal/Administrator.* ● *The IP address of the computer used to login is*	**Oftentimes, incidents like this occur because systems are misconfigured or misused. That is the case with how this business is sharing information among its employees. My notes in short:** ● *Robert Taylor Jr is an admin.*	**It appears as though a former employee is potentially the threat actor. However, it's possible that they were not the person responsible for this security incident. It is common for people to reuse login credentials across many services. And if those credentials are compromised on one platform then an attacker can use them to gain access to others. In this case, implementing access controls, like password policies, limited file permissions, and MFA can protect the business from**

	Note(s)	Issue(s)	Recommendation(s)
	152.207.255.255.	● *His contract ended in 2019, but his account accessed payroll systems in 2023.*	**incidents like this.** **My recommendations as follows:** ● *User accounts should expire after 30 days.* ● *Contractors should have limited access to business resources.* ● *Enable MFA.*