Access Controls Summary

Objective:

Investigate unauthorized access to payroll system.

Case Summary:

- Attacker accessed payroll from IP 152.207.255.255 using a computer named Up2-NoGud
- The account belonged to former contractor “Robert Taylor Jr”, whose contract ended in 2019
- Access level: Administrator

Issues Identified:

- Orphaned account still active
- Admin-level permission granted to temporary contractor

Recommendations:

- Enforce user lifecycle management (disable expired accounts)
- Enable multi-factor authentication (MFA)
- Apply least privilege principle for all contractor accounts **Framework Mapping**:
- NIST AC-2 (Account Management)
- NIST AC-6 (Least Privilege)

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident? Acces form IP 152.207.255.255* ● *When did it occur? Date: 10/03/2023, Time: 8:29:57 AM* ● *What device was used? Computer: Up2-NoGud*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have? Robert Taylor Jr is an Administration* ● *Should their account be active? No. His contract ended in 2019, but his account accessed payroll systems in 2023.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* *- Deactivated payroll account for expired contractor* *- Enable multi-factor authentication (MFA).* *- Contractors should have limited access to business resources, don't give Administration authorization.*