

Access Control Worksheet

Scenario: You're the first cybersecurity professional hired by a growing business. Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn't make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents. To do this, you'll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	Objective: List 1-2 pieces of information that can help identify the threat: <ol style="list-style-type: none">1. <u>Who caused this incident?</u> Administrator.2. <u>When did it occur?</u> 10/03/2023.3. <u>What device was used?</u> Up2-NoGud. The IP address of the computer used to login is 152.207.255.255.	Objective: Based on your notes, list 1-2 authorization issues: <ol style="list-style-type: none">1. <u>What level of access did the user have?</u> Administrator. It is Robert Taylor Junior.2. <u>Should their account be active?</u> No. His contract ended in 2019, but his account accessed the payroll system in 2023.	Objective: Make at least 1 recommendation that could prevent this kind of incident: <ol style="list-style-type: none">1. <u>Which technical, operational, or managerial controls could help?</u><ul style="list-style-type: none">• User account should expire after 30 days.• As contractors, they should have limited access to business resources.• Multi-factor authentication is needed.

Event Type: Information
Event Source: AdsmEmployeeService
Event Category: None
Event ID: 1227
Date: 10/03/2023
Time: 8:29:57 AM
User: Legal\Administrator
Computer: Up2-NoGud
IP: 152.207.255.255
Description:
Payroll event added. FAUX_BANK

[illegible]