

Access controls worksheet

Eliyas Philip

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	<p>Objective: List 1-2 pieces of information that can help identify the threat:</p> <ul style="list-style-type: none">• <i>The attacker had legal/admin rights through using employee account.</i>• <i>Occurred on 10/03/2023 at 8:29:57 AM.</i>• <i>The device had a strange name.</i>	<p>Objective: Based on your notes, list 1-2 authorization issues:</p> <ul style="list-style-type: none">• <i>The user had admin access.</i>• <i>The account shouldn't have been active, it was supposedly closed over 4 years ago.</i>	<p>Objective: Make at least 1 recommendation that could prevent this kind of incident:</p> <ul style="list-style-type: none">• <i>First close the account and remove any admin rights from accounts not being used anymore. Do routine checks of user activity and access.</i>