

Access controls worksheet

	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">● IP: 152.207.255.255● DATE: 10/03/2023● TIME: 8:29:57 AM● Machine: Up2-NoGud● EVENTID: 1227 <p>The event occurred early in the morning and it seems to be from an authentication user.</p>	<p>Objective: Based on your notes, list 1-2 authorization issues:</p> <ul style="list-style-type: none">● Level Access: Not Admin● Status: Inactive <p><i>The access seems to be from a former employee of the company who left the company in 2019.</i></p>	<p>Objective: Make at least 1 recommendation that could prevent this kind of incident:</p> <ul style="list-style-type: none">● <i>Audit employees credentials usually and block the access to former employees</i>● <i>Revoke all access to credentials with end date expired</i>