Date: 3/21/2024	**Entry: 5**
Description	This journal entry provides details about investigating failed SSH logins for the root account on the mail server at Buttercup Games.
Tool(s) used	Splunk Cloud and Network Protocol Analyzer
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was caused by unauthorized attempts to log in to the root account on the mail server. ● **What** happened?Multiple failed SSH login attempts were detected for the root account on the mail server. ● **When** did the incident occur? The incident occurred during the period of investigation, specifically within the timeframe of data analysis. ● **Where** did the incident happen? The incident happened on the mail server of Buttercup Games. ● **Why** did the incident happen? The incident likely occurred due to malicious actors attempting to gain unauthorized access to the mail server by targeting the root account.
Additional notes	- The investigation revealed over 100 failed SSH login attempts for the root account. - Further analysis is needed to determine the origin and intent of the unauthorized login attempts. - Recommendations include implementing stronger authentication measures and monitoring for suspicious activities on the mail server.