Scenario 1:

Date: November 05, 2024, 07:18 a.m.	**Entry:** 1
Description	The investigation focuses on identifying patterns or malicious behaviour related to failed SSH login attempts targeting the root account on the mail server.
Tool(s) used	- **Splunk**
The 5 W's	- **Who:** A malicious actor attempting unauthorized access to the root account. - **What:** Multiple failed SSH login attempts were detected on the mail server, raising concerns of a possible brute-force attack. - **Where**: The incident was identified at Buttercup Games, an e-commerce company. - **When**: The activity occurred between October 24, 2024, and November 4, 2024. - **Why**: The attacker appears to have been attempting to gain unauthorized access to the company's mail server, likely to steal sensitive data or install malicious software.
Additional notes	To identify failed login attempts, the following search query was used in Splunk: `index=main host=mailsv fail* root` This query retrieved all events with variations of the word "fail" (e.g., failed, failure) and associated them with the root account on the `mailsv`

	host. **Findings:** 346 failed SSH login attempts for the root account were recorded during the specified time frame.

Reflections for Scenario	This scenario highlights the importance of monitoring critical systems for suspicious activities. Regular log analysis and the implementation of proactive security measures, such as multi-factor authentication and access restrictions, can help prevent similar incidents in the future.

Follow-Up Actions	**Analyse Logs Further:** Review the `fast.log` and `eve.json` outputs to identify IP addresses and geolocations associated with the failed login attempts. **Implement Mitigation Measures:** • Block suspicious IP addresses identified in the logs. • Enforce stronger password policies for root accounts. • Restrict SSH access to the mail server using IP whitelisting. **Monitor for Further Activity:** Set up Splunk alerts to notify security personnel of unusual login attempts in real time.