Incident handler's journal

DATE->(DD/MM/YY)

Date: 18/09/23	**Entry: #3**
Description	Security analyst was hired by e-commerce store ‘Buttercup Games’ to screen for any possible security issues within the mail server. Exploring the information within the SIEM(Security Information and Event Management) tool revealed over 300 failed logins between 27/02/23 and 06/03/23
Tool(s) used	SIEM tool ‘Splunk’
The 5 W's	Capture the 5 W's of an incident. ● **Who** => It’s unknown who may be doing this as the ip addresses are constantly changing, additional monitoring is needed ● **What** => 346 failed login attempts ● **When** => Between 27/02/23 and 06/03/23 ● **Where** => mailsv1 ● **Why** => Appears to be a potential brute force attach on the SSH channel, cause and motive is unknown except for knowing that the attacker is attempting to gain access to a privileged account(root)
Additional notes	So far, it’s only been failed attempts so nothing damaging has happened yet, ensure that the password policy and MFA is updated and running to reduce the chances of a potential breach