Use case written on the Splunk

When Conditions are met- Alert triggers.

Alerts are forwarded on to Monitoring tool

L1 Analyst assigns the alert to his name and starts to investigate

Alert Triggers when there are more than 10 failed login attempts followed by a successful login.

- Check the Frequency of failed login and intensity of the attack.
- Check if the User has changed the password recently.

Analyse the logs to see

1. the reason for login failure.
2. Log – on type.
3. Status Code and Sub-status code.
4. Check if there is a process involved in failed login attempt.

Analyse the Source IP attempting to log in to our network.

1. Check the reputation of IP in TI tools.
2. Check the country to which the Ip belongs (whois lookup)
3. Compare the IP of regular login activity with the filed login attempt IPs

- Block the Source IP(Attacker IP) on Firewall, by raising the INC on SNOW to NOC team.
- Clear the browser data if any passwords are stored.
- If there was a successful login after high number of failure login – Disable the account temporarily and Change the password of the user by raising the INC to AD team