Splunk Use Cases from Logs

1. Detection of Repeated Access from a Suspicious IP

2. Access to Restricted Ports

3. Firewall Rule Mismatch

4. Multiple NAT Rule Hits

5. Traffic from Blacklisted IP Ranges

6. Incomplete Log Entry Detection

7. Protocol Misuse Detection

8. High Volume Traffic to Specific Destination

9. Unusual Internal to External Access

10. Same Source Port Reuse Across Sessions