### **Report 1: RDP Brute Force Attack**

**Title**: Successful RDP Brute Force and Post-Exploitation Enumeration  
**Date**: May 30, 2025  
**Platform**: Let’s Defend SOC Simulator  
**Severity**: Medium  
**Detection** Tool: Chronicle SIEM  
**Category**: Authentication / Remote Access

**Steps Taken:**

* Investigated authentication logs in Chronicle SIEM
* Observed numerous failed logins using common usernames (e.g., admin, guest)
* Noticed eventual successful login with valid credentials
* Scanned source IP (218.92.0.56) in VirusTotal
  + Flagged as malicious on VirusTotal
  + GeoIP traced to China
* Post-login commands executed by attacker:
  + net user letsdefend
  + net localgroup administrators
  + netstat -ano

**Final Assessment:**  
**True Positive**. A brute-force RDP attack led to unauthorized access, followed by reconnaissance activity. Attacker successfully enumerated user and network information.

**Mitigation:**

* Immediately isolate the compromised host from the network
* Block the source IP at the firewall and implement country-based IP restrictions
* Enforce strong RDP access controls, including:
  + Account lockout policies
  + Multi-Factor Authentication (MFA)
  + Limited RDP access via VPN
* Review logs for lateral movement or persistence
* Reset credentials for affected accounts