**SOC Daily Activity Report**

**Analyst Name:** Posaram Dewasi  
**Date:** 07-Sep-2025

**1. Reviewing Security Alerts & Logs**

* **Log Source:** Windows Event Viewer → Security Logs
* **Event IDs Observed:**
  + 4625 → Failed Logon
  + 4624 → Successful Logon
  + 4798 → User Group Enumeration

**Example Finding:**

* Multiple failed logon attempts (Event ID 4625) observed for user rajiv.kumar.
* Source Network Address: 192.168.1.50
* Logon Type: 3 (Network Logon)

**2. Investigating & Responding to Incidents**

* Collected evidence using Event Viewer filters and PowerShell commands:
  + wevtutil to export logs
  + netstat -ano to capture active network connections
  + tasklist /v to capture running processes
* Compressed evidence to archive for escalation (evidence.zip).

**Observation:**  
Suspicious failed logins suggest a possible brute-force attempt.

**Action Taken:**

* Saved logs for escalation.
* Recommended blocking suspicious IP and resetting user password.

**3. Updating Threat Intelligence**

**Indicator Analyzed:**

* Source IP: 192.168.1.50

**Threat Intel Findings:**

* VirusTotal: Flagged as malicious by multiple vendors
* AbuseIPDB: 25 abuse reports (Brute Force activity)

**Action Taken:**

* Updated internal blocklist (theoretical)
* Documented indicator in threat intel report

**4. Collaboration with Team**

**Escalation Note:**

* Shared findings with L2 SOC Analyst
* Evidence archive and screenshots attached
* Requested IR team to block malicious IP and investigate lateral movement

**5. Threat Hunting Activity**

**Hypothesis:**  
Attacker may be attempting brute-force login across multiple accounts.

**Findings:**

* Same IP (192.168.1.50) attempted logins on 5 different accounts
* Successful logon (4624) occurred after multiple failures
* Group enumeration (4798) observed post-login

**Observation:**  
Pattern indicates brute-force attack followed by privilege reconnaissance.

**6. Training & Continuous Learning**

**Training Performed:**

* Completed TryHackMe SOC Level 1 labs
* Practiced Splunk for Windows log analysis
* Learned Sysmon advanced logging basics

**Threat Intel Awareness:**

* Subscribed to AlienVault OTX feed
* Read The Hacker News article on recent RDP brute-force attacks
* Reviewed recent CVEs related to Windows authentication